ERICSSON


# TIME TO PRESS THE GO BUTTON

# CONTENTS

# PAPER 2 REVISITED


# INTRODUCTION

The world's largest enterprises have not adopted cloud, 74% are concerned about cloud security and governance and 67% don't have the cloud IT expertise [ref: Cloud Connect and Everest Group "Enterprise Cloud Adoption Survey 2014"]. If you are a large enterprise or you wish to provide cloud services to large enterprises this paper is for you.

Change in the world is not slowing down (See "Changing the Game") and seeing the world differently is more valuable than ever (See "Winning the Game.").

This is the third paper in a series. This paper focuses on changes now happening, and taking part in those changes – from a user and from a provider perspective.

The second paper ended with a discussion of the need to create the digital shipping system. Any system which moves goods from one place to another requires predictability and performance in order to accelerate growth. In the physical shipping industry, these were achieved with the invention of the shipping container, its associated shipping manifest detailing its contents, and the creation of specialized ports and ships to handle containers.

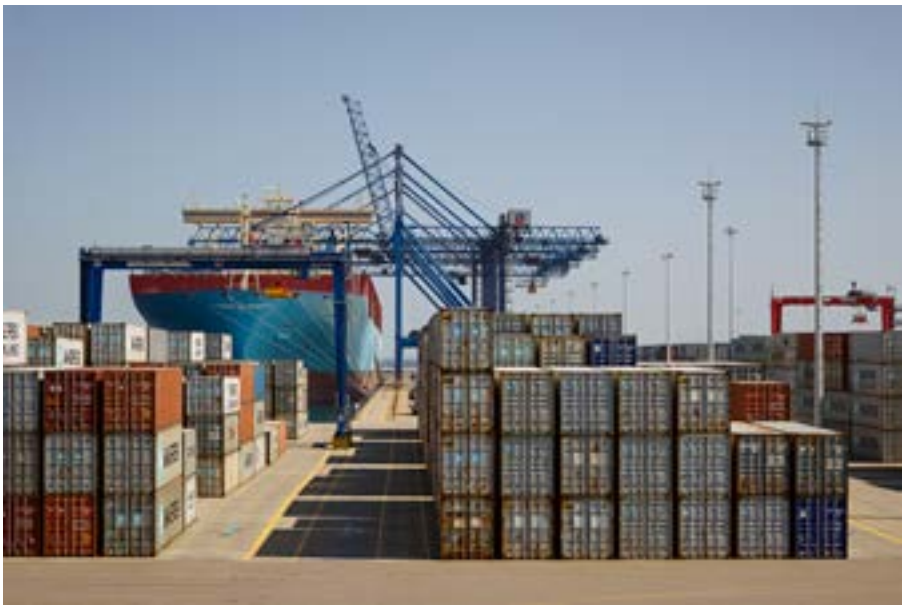
This paper introduces the network as analogous to the ship moving the data, the cloud as the port handling all data, and any data object wrapped with immutable meta-data as the shipping container and its contents.

A second and arguably even more important change brought about by the shipping container was the elimination of theft and fraud. The containers were secured and tamper proof. Similar protections will be needed for the digital shipping system: data needs to be stored and shipped in such a way that it cannot be tampered with, altered, or diverted.

The World Economic Forum predicts that big data, its associated analytics, and cloud will create 21.6 TR USD in value for the global economy by the end of this decade – contingent on the availability and deployment of the right kind of infrastructure.

If your business is dependent on data you can trust, then you need data infrastructure you can trust. If you provide the data infrastructure from communications (network) to storage to management (cloud), then you need provide service that is forensically auditable and provable by a third party.

The Networked Society is happening. It changes everything. As William Gibson famously said: "The future is already here, it's just not very evenly distributed." Welcome to "The Game Has Changed – Time to Press the GO Button"



The game has changed – time to press the go button

# INTERNET OF THINGS

During 2008, the number of things connected exceeded the number of people on the planet. By 2020 it is predicted that 50 billion objects will be connected, seven times more than the number of people. This trend is only expected to accelerate in the future.

Why?

Devices are being connected for the information they know, the change they can effect, and the experiences that can be provided from both.

Since the beginning of time, information has enabled progress. The collection of information was challenged by the physical properties of distance and time, which slowed the ability to decide and act. Telecommunications have always removed time delays and speeded up decision-making – hence their innate value to a developing world. Faster information has always enabled better decisions and better actions.

The telegraph station was step one: it required specialist buildings. It was superseded by the fixed-line telephony network, which connected approximately one billion "general" buildings worldwide. This, in turn, was superseded by the mobile telephony network, which has connected approximately six billion people to date. The next natural progression is to connect… everything else. Ericsson calls this "the Networked Society."

The previous generations of technological change were all about enabling humans to communicate with humans. In the Networked Society, for the first time, machines will be speaking to machines, as well as to humans. They will be speaking by sharing data. The machines will be able to analyze the data very quickly, make their own decisions and take action, all without the direct involvement of people. People will begin to focus on programming the machines to make better, faster decisions, rather than people making the decisions themselves.

## Distance and time will trend to zero

Distance and time will trend to zero: anything, anywhere will be shared, as if all interested parties are in the same location at exactly the same time.

This will transform how businesses make decisions: increasing efficiency, enabling new services to be offered, and creating new experiences.

There are clear benefits. Efficiency of resource use is maximized. The opportunity to create more tailored and better experiences is increased. And, businesses that are more efficient and innovative can be more successful. For the first time in history, the three dimensions of profit, planet, and people can be addressed without compromise to one or another. Ericsson calls this the "Triple Bottom Line"

The future must work on data that can be trusted. For any data, we

### Networked Society Explained

need to know: Where did it come from? Was it changed along the way? Is it still the same as it was one minute ago? One hour ago? One day ago? One year ago? One hundred years ago?

All businesses operate on data. Business decisions based on data are investments, whose worth has been decided based on projected risk and return. The more granular and recent the data used to make such decisions, the better risk can be managed, the better the investments made, and the better the return received. This is true for operating decisions, and also for decisions about new markets and services.

Historically, decision-making data has been collated from the past, generalized, and of low granularity. Today, the data available from all devices connected provides up-to-date, very precise information: situational awareness. For example, Google has better real-time predictions on the global status of the flu virus than the World Heath Organization does (http://google.com/flutrends).

The quality of decisions and the ability to trust them will be based on the quality of the data used in making them, and the level of trust that can be placed in that data. Today, there is no chain of custody, integrity, or attribution of history to data. There is no awareness of tampering, and there is clearly no belief that data cannot be reached by malicious parties: every day we learn of a new data breach.

The Networked Society requires an infrastructure with inherent real-time attribution, forensic, and auditing capabilities. Data needs an immutable shipping manifest that can be independently verified as true and can offer forensic information in real time if compromise is discovered.

It is impossible to prevent 100% of all data crime. It is possible, however, to detect 100% of crime – and act accordingly.

The quality of decisions and the ability to trust them will be based on the quality of the data used in making them, and the level of trust that can be placed in that data.

# SOCIETY NEEDS SECURITY, DATA NEEDS INTEGRITY

In a world driven by “as fast as possible” decisions, it is important to be able to trust that data, have immutable proof of that data’s history, and have the forensic and auditing capability to understand what happened to the data if something goes wrong.

Today, data security is over-reliant on encryption and access, both of which have proven to be false safe harbors. Both depend on the integrity of the underlying systems, and the need to trust the people operating them. Both of these dependencies are not reliable.

Mike Rogers, chair of the US House Intelligence Committee, says that 95 percent of private sector networks are vulnerable to cyber attack, that most have already been hit, and that people working inside the organizations cause between 30 and 50 percent of the security breaches. Trust is proving to be not enough of a safeguard.

The CEOs who believe that they have not experienced compromise have simply not yet discovered the cancer.

In order to foster growth, industries and countries need a predictable and deterministic environment, where risk can be managed alongside investment and return. The World Economic Forum believes that the lack of effective cyber security could cost as much as USD 3 trillion in non-realized potential growth during this decade.

Industries need to ensure that their data has high integrity – and can be validated as such. For this to be true, any used cloud must have data life cycle management as a fundamental capability, designed and built into its infrastructure and operation.

Data life cycle management consists of attribution at source, real time situational awareness with native forensics and auditing capability that can be performed by an independent third party.

The result – data integrity secured with truth – is the only way to maintain trust in a system.

Mechanisms now exist where proof is based on well-known public mathematics that can be independently verified. An independent third party can irrefutably validate governance and compliance, – without the need to disclose the source data. There is no need to ever trust any messenger again, especially not a messenger who may have another vested interest.

This becomes increasingly important as the world moves towards using cloud infrastructure, which by nature is highly available

People working inside the organizations cause between 30 and 50 percent of the security breaches. Trust is proving to be not enough of a safeguard.


and shared. The economics of the cloud are driving companies to use such approaches, but those that do so without data integrity instrumentation will find themselves in a world more similar to the Wild West than Wall Street.

At a fundamental governance level, such instrumentation should be required as a basic component of business operation. This will enable society to reap the benefits of sharing, while at the same time creating a more secure environment than exists today. The World Economic Forum describes three possible future scenarios:

1. The world continues muddling into a future in which attackers are increasingly effective against under-tooled and less-agile target organizations.
2. There is a backlash against digitization, causing fragmentation and stunted growth.
3. There is accelerated digitization, thanks to robust cyber-resilience.

The definition of what is required to enable option 3 (accelerated digitization) can be summarized in four parallel tracks:

1. Cost savings through adoption of shared infrastructure and associated economics. This increases complexity, especially when compliance and forensics are a prerequisite
2. Subsequent security challenges. Placing data in shared infrastructure and making it easier to access is good economically, but also enables others who should not have access to do the same.
3. Management of plaintiff litigation, e.g. lawsuits from individuals who have been compromised due to breach, or similar lawsuits from other companies (subrogation).
4. Total cyber governance, where company officers have a basic fiduciary duty to oversee the risk management of their company, which includes securing any intellectual property and trade secrets.

To reference Matthew Johnson, a world-leading cyber security expert and CTO of Guardtime, at a recent keynote in Asia:

For these multinationals, outsourcing business trust to the largely unregulated cloud service provider industry today (regardless of the contract guarantee) ultimately belies the belief in the constraints on that provider's trusted insiders (and, indeed, any

## Accelerated digitization thanks to cyber resilience

government) interactions with your data, as well as the integrity of purported technical security controls, abeyance of best practices, and associated policies and processes.

While CSA and world standards bodies have pioneered a number of policies and best practice tenets to manage cloud computing and data risks and security threats, these best practice frameworks for business, organizations, and governments are merely a risk management framework which does not address very fundamental integrity problems or technology solutions that should be associated with cloud models.

We should begin to change the dialog and emphasize…

- CIOs should make the assumption that any outsourced infrastructure will at some point be compromised (if not already).
- You can't outsource trust with the complexities offered today or with the people operating those resources on your behalf.
- Also assume your own internal infrastructure is already compromised or soon will be in the (near) future.
- The more important and valuable your intangible assets are (your intellectual property, customer and supplier base, etc.), the more likely you are to be compromised and to become – no pun intended – a TARGET.
- The siren song has become, 'We implement best practices!!' to assuage concerns.
- Our response has always been, 'So prove it in a way I can independently verify the integrity of your systems any time I want' – go beyond compliance. Prove it. Prove in an independently verifiable way that the integrity of my data, the information rules that govern it, and that my service contract is being enforced – and let me do it whenever I want – in real time.

With these assumptions, guaranteeing the integrity of these machines, the data being generated both by them and the user, and the rules used to enforce the information policies and contracts is paramount.

With integrity guarantees, true cyber security for an organization is possible.

Ericsson is architecting its infrastructure with integrity first, to enable the vision described above: a risk-managed, commerce-first infrastructure and operation that can be governed, can be proven to be compliant by third parties, and to have real-time situational awareness on all assets and integrity.

We should begin to change the dialogue and emphasise...

# FORENSICALLY AUDITABLE INFRASTRUCTURE FOR CLOUD AND BIG DATA

Business is investment, and investment is the management of risk.

"The ability to define what may happen in the future and to choose among alternatives lies at the heart of contemporary societies. Risk management guides us over a vast range of decision-making, from allocating wealth to safeguarding public health, from waging war to planning a family, from paying insurance premiums to wearing a seatbelt, from planting corn to marketing cornflakes." [Against the Gods]

Those who can better predict the future will always make better investments. The foundations of modern business have been: asset management (the investment of assets into growth), business auditing (guarantees that businesses are compliant to what is expected), and insurance (the coverage of investment when unexpected events occur).

Since the 17th century, the combination of these industries has led to the exponential growth of business: for the first time, there was a level of predictability in the future, and predictability enables investment with the expectation of growing returns.

Those who predict the future most accurately have always had access to better data on which to base their predictions – data that has traditionally been historical and statistically valid over large populations.

Both the insurance and auditing industries have managed risk in a relatively static way, because the source data used to assess and the processes used to audit risk have been relatively static.

The fundamental change to business today is the movement of knowledge of the future away from static actuary tables and towards real time data.

The fundamental change to business today is the movement of knowledge of the future away from static actuary tables and towards real time data. Risk becomes a function, not of what has happened on average over years, but of what has actually happened the second before right now, at an individual, device, and company level.

Those who continue to manage generalized historical risk will never make investment decisions equaling the insights of those who can manage risk right now on a very granular level.

Traditional asset management organizations are very aware of this disruption, and are understandably questioning the future of their industry – "Tech Giants pose Threat to Fund Houses" [FT].

Simple examples: Google can now predict what you will click before you click it. They also know the state of global flu right now [Google Flu]. Amazon has patented the process behind delivering goods before you have even ordered them.

As the world moves towards everything being connected, the businesses of investment, insurance, and auditing need to wake up: risk is no longer a function of the past, but a property of the veracity of data right now.

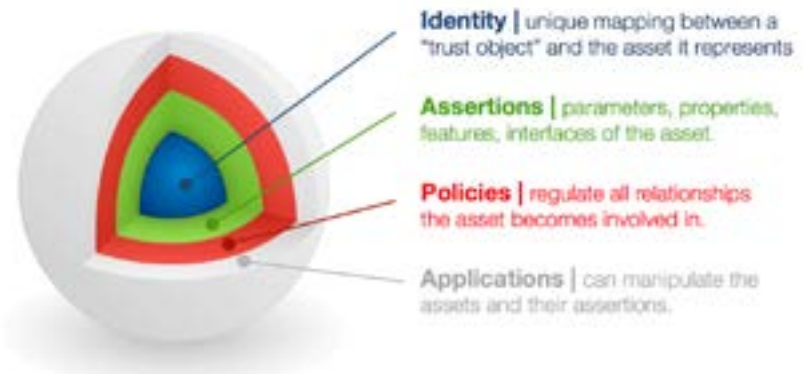
Because investment, insurance, and auditing enable all business, all of these industries need to change to manage the new future. Because businesses provide wealth to countries, all countries need to change to manage their future GDP. Because all countries trade with other countries, all international commerce has to change. [FT]

If the data used to make decisions cannot be shown to have mathematically verifiable history and integrity, then the decisions cannot be trusted, and compromise can occur, to the detriment of the companies involved, their investors, their shareholders, and their auditors. What to do? Key to understanding how to secure this future is to understand the paradigm shift: treat everything in the digital economy – server software, configuration files, log files, business information in any format – as a data object. Than all can be given attribution and integrity through signing at scale. Any change occurring anywhere can then be identified in real time, and signaled as either expected – or not, and therefore likely compromised.

## Treat everything in the digital economy ...as a data object

The Networked Society is dependent on the independent confirmed veracity of the data it is using to manage risk. The previous chapter highlights the challenges in this scenario. This is why cyber crime and cyber security is the battleground of future economic growth and prosperity. This sounds dramatic, but it is simply the truth. Lose control of your data as a person, as a company, or as a country – and you lose control of your future.

## Sleep At Night



# BIG DATA GOVERNANCE

Forbes was the first to coin the term "Data Lake" in a 2011 article: "Big Data Requires a Big, New Architecture." The difference between a data lake and a data warehouse is that data coming into a warehouse is sorted and pre-categorized upon entry into a data warehouse. The logic of the data lake is that there is no analysis on data ingress, enabling more flexible analysis afterwards. There are ongoing debates as to which approach is more effective and appropriate.

However, neither approach addresses the governance required to ensure that any result and conclusion drawn from the data has veracity and trustable value.

All data needs to be managed with transparency, traceability, and integrity, both source data and any resulting generated data. Data needs to be tagged, tracked, and located, such that a third-party auditor can prove compliance without compromising confidentiality.

Here we introduce the concept of a "data bank" that manages data in the same way that a financial bank manages money, with built-in compliance, governance, traceability, integrity, and scale.

Data Bank = (Data Lake or Data Warehouse) + Governance

The history of data and where it is stored are becoming a national debate in nearly all-modern countries. The Data Bank enables commercial entities to enjoy the economic efficiencies of shared mass storage, while at the same time inheriting the benefits of a transparent governance operating model, in multiple countries, obeying government and industry regulations specific to each.

People and companies who have a lot of money do not build their own bank. They place it in an existing bank where it is known to be safe, secure, and trusted. This bank is part of a larger network of banks that enables seamless trade.

The same should be true for data. Data should be placed in a data bank to reduce crime, increase trust, and drive economic savings and growth. Orchestration of different data banks and their interworking should be seamless, to enable digital trading with trust, compliance, and transparency.

## DATA IS THE NEW OIL

- Who Owns it?
- Where is it?
- Who regulates it?
- Who garantees it?

# IN SUMMARY

The world's largest enterprises are looking for cloud providers that can offer governance and security.

In order to foster growth, industries and countries need a predictable and deterministic environment, where risk can be managed alongside investment and return. It is premised on industrial grade infrastructure and the creation and use of subsequent data that can be trusted, used, and traded.

The world's largest enterprises are looking for industrial grade infrastructure, industrial grade providers and industrial grade governance and process. Industrial grade is synonymous with "telco grade" for telco.

All data needs to be managed with transparency, traceability, and integrity, both source data and any resulting generated data. Data needs to be tagged, tracked, and located, such that a third-party auditor can prove compliance without compromising confidentiality.

Contact your local Ericsson representative for more information, or email:

Geoff Hollingworth
geoff.hollingworth@ericsson.com

Jason Hoffman
jason.a.hoffman@ericsson.com

The game has changed. It is now time to press the GO button…

Ericsson AB
SE-126 25 Stockholm, Sweden
Telephone +46 8 719 0000
Fax +46 8 18 40 85
www.ericsson.com

EN/LZT 000 0000 000