

TRUST CHALLENGES AND ISSUES

TRUST IN

DIGITAL LIFE

DATE: 02/7/2010
VERSION: V1

Secure e-Solutions[®]

GMV SOLUCIONES GLOBALES INTERNET S.A.

UNCLASSIFIED INFORMATION

The information contained in this document has been classified to a level of "Unclassified", according to GMV Soluciones Globales Internet S.A.'s Information Security Management System (ISMS). This classification allows its receiver to use and redistribute the information, making reference to the source of the information; observing legal regulations in intellectual property, personal data protection and other legal requirements where applicable.



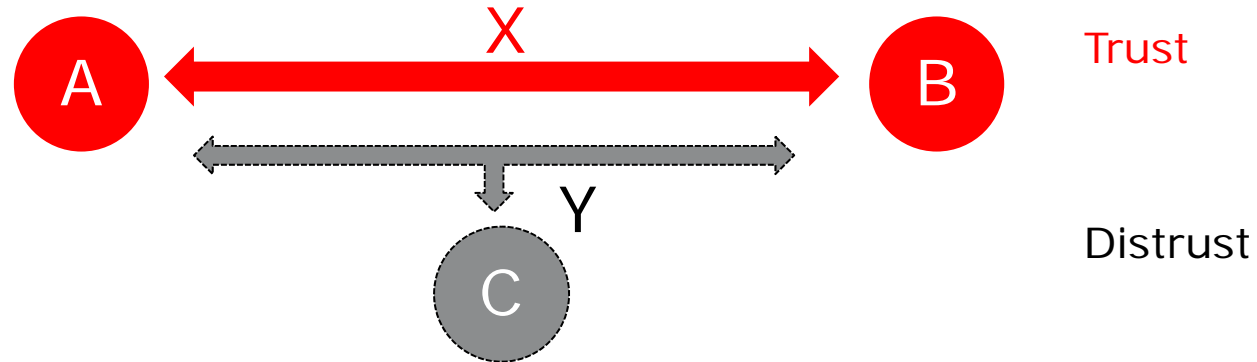
INTRODUCING GMV

- Multinational industrial group founded in 1984. Private capital
- > 1.000 employees all over the world
- Currently operating in
 - Aeronautics
 - Space
 - Defense
 - Security
 - Transportation
 - Healthcare
 - ITC industries
- Subsidiaries/offices in 7 countries
- > 20 years in cooperative European R&D efforts



TRUST & TRUSTWORTHINESS

- Trust: subjective & context related



- Trustworthy systems & services
 - Secure
 - Reliable
 - Resilient to attacks & operational failures
 - Protecting user data
 - Ensuring privacy
 - Providing usable & trusted tools to support the user in his security management



CARBON (NON SILICON) DIGITALLY AUGMENTED LIFE

- Dealing with people:
 - Risks to e-trust are not a mere IT systems incident or avatars affairs
 - “Revolution does not happen when society adopts new technology, it happens when society adopts new behaviors” C. Shirky
 - Dynamics of change. Education & awareness to assess new risks scenarios
 - Usability, a feature for success



Question 20th

Among the following, please answer the main reason why you have never used electronic transactions with Public Administration throughout Internet. And in second place?

	MAIN	SECOND
I rather have a printed and sealed copy of my files	10.1	10.8
I mistrust the security of personal data on the internet	11.0	11.0
The information available online provided by Public Administration, is insufficient	1.9	2.7
I rather consult in person	25.0	17.1
The electronic requirements for online procedures are complex. (electronic ID)	4.6	6.0
On the internet I can't keep track of my procedures' status.	.5	2.3
I wasn't aware of the possibility of online procedures (DO NOT READ)	2.8	1.7
I don't know how to use internet (DO NOT READ)	22.2	14.1
I don't have internet access (no computer, no Internet connection) (DO NOT READ)	14.0	11.6
Other answers	3.0	1.8
Doesn't know	1.7	11.8
No reply	3.2	9.0
(N)	1422	1422

SOURCE: CIS BAROMETER
March 09

INCREASING LINKS BETWEEN “REAL” & “DIGITAL” WORLDS

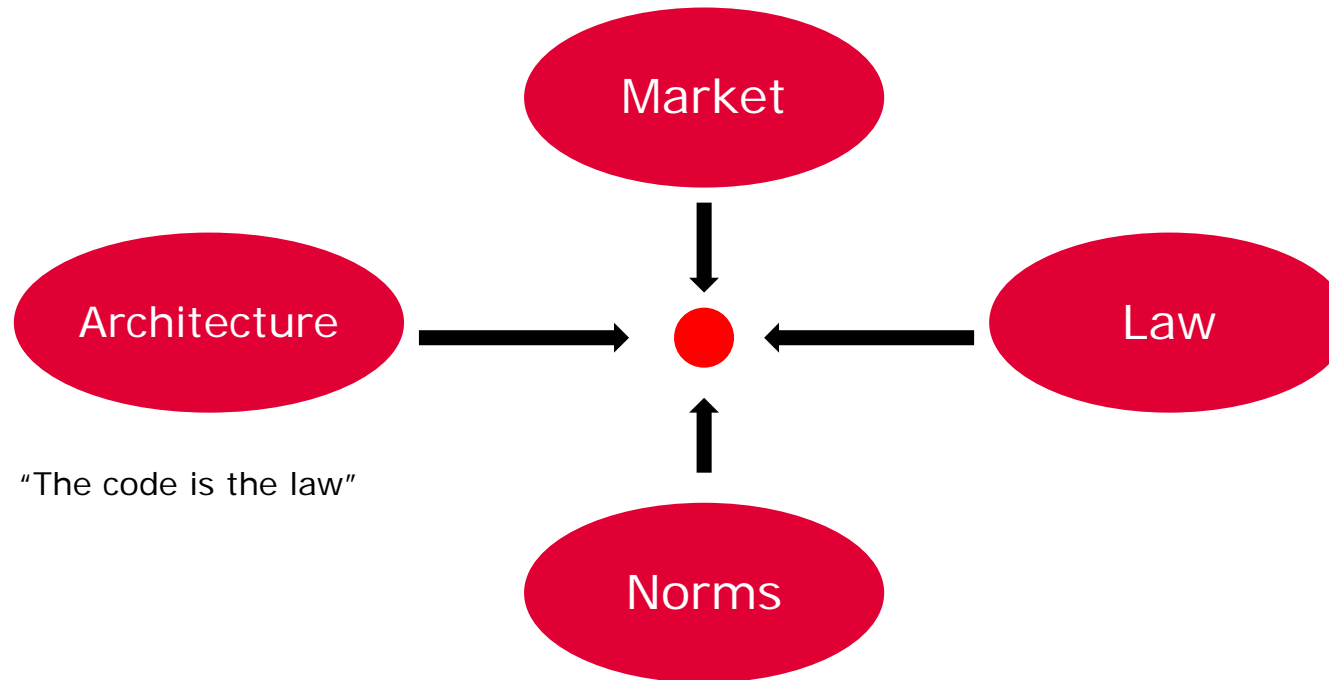
- For people, business & governments
- “Internet of things”
- Physical & logical security convergence
- Pervasive environments
- Law enforcement must be improved on an international basis
- Location-based services

- Galileo: trust as an added value
 - European (autonomous) extremely precise source of navigation and time distribution
 - Anti-spoofing (signal authentication) mechanisms
 - Integrity:
 - guaranteed (very high probability) bounding of position and time errors:
 - An essential feature in Liability Critical applications in which the use of position/time has legal/economical implications



REGULATION IN INTERNET

- L. Lessig: four forces (“regulators”) constraining users ability to do things



- Historical shift in power: architecture > market > law
- Very likely, towards a highly controlled internet
 - Strong arguments from global security concerns, incidents in Internet will provide for the required activation energy
- Is it desirable from (we) citizens point of view?:
 - Freedom is granted by law / privacy can only be protected by law....
- ... and the remaining regulators should support it

PRIVACY BY DESIGN

- “(Privacy) Law is the code” (?)
- Principles (IPC Ontario):
 - Proactive, no reactive; Preventive not remedial
 - Privacy as the Default
 - Privacy Embedded into the Design
 - Full functionality, positive sum, not zero sum
 - End to End lifecycle protection
 - Visibility and transparency
 - Respect for user privacy
- Privacy by design comprises IT systems, business practices, physical design & infrastructure
- Privacy attributes: anonymity, pseudoanonymity, unlinkability, unobservability
- Total anonymity and untraceability will not happen, both from legal and commercial constrains. Privacy must coexist with control requirements
- Very often, too much focus on data exchange, forgetting data protection
- Some threats, from internal & external attackers:
 - Information leakage
 - Pervasive environments
 - Physical & logical surveillance
- Our views on respect for privacy will not be shared by all international commercial & governmental agents.
- User education is fundamental
- Some recent practices in social networks: privacy center
- Standardization efforts required
- Usability: e.g. marks similar to intellectual property licensing for privacy homogeneous spaces



IDENTITY MANAGEMENT

- A core issue of trust
- Identity layer, the reflection on architecture: towards a flexible and user centric ID management
- European interoperable infrastructure approach:
 - Federated
 - Multi-level
 - Relying on authentic sources
 - Permitting a context or sector based approach
 - Enabling private sector uptake
- Fuelled by services directive & Relevant European supporting R&D efforts
- Despite technological neutrality:
 - most widespread solution is PKI certificates inside intelligent cards
 - mobile phones relevant role
- eDNI experience:
 - usability & services/devices availability & virtuous cycle
 - change needs resources but also time & education & incentives
- Adoption by private sector is a key success factor. Role of financial & telco services
- Are users interested? Which are their incentives vs. perceived barriers?
 - e.g. fraud, theft, impersonation risks vs privacy concerns
- Identity providers/intermediaries, concepts to be further developed
- Further development of open standards
- Together with infrastructure, legislation must be further harmonised
- On the security side of trust too much emphasis is put on user authentication, leaving aside the fact that end-to-end security is required
- Trust is subjective and context related, e.g virtual communities

WEATHER FORECAST: CLOUDY

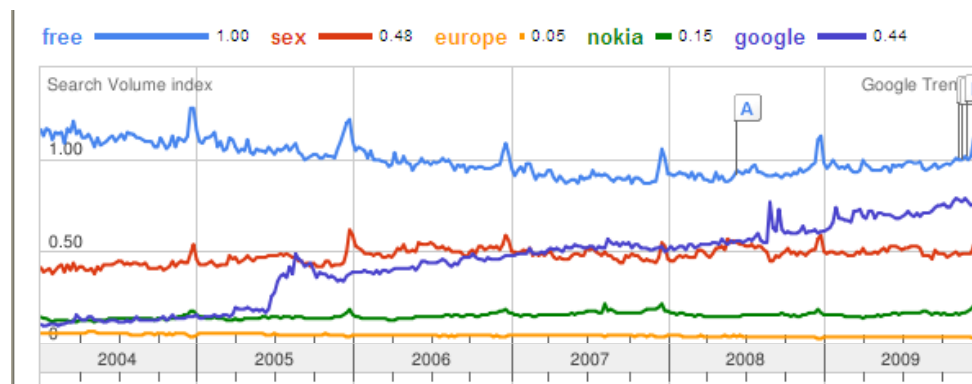
- A major shift: data from users equipment or servers to the “cloud”
- A (relatively) new trust scenario, key issues: service levels, providers location and providers trust
- A new trade-off (Enisa 2009)



- Barriers to cloud (opencloudmanifesto.org): Security, Governance and Management, Metering & Monitoring, Data & Application Interoperability and Portability
- A new argument for Information Governance in organizations
- More than a new architecture:
 - A new business proposal
 - A shift in market power: new agents, different providers localization
- Europe must build its place in this new scenario:
 - In terms of business (not only ICT industry)
 - Protection of European citizens data

“FREE” BUSINESS MODELS

- Negligible marginal costs in digital goods & services have raised the case for “free” as an arguable business or service provision model
- The “blessings”:
 - Free & virtually unlimited (legal) access to digital contents
 - 2.0 phenomena of collaboration
 - Legitimate new business models, e.g. open source software, “freemium”, consumer communities building, etc
- The dark side:
 - Illegal behavior wrt digital property rights
 - Obscure business models & value proposal: TNSTAAFL
 - Very often, user’s data as a hidden price
 - Cultural shift:
 - Perception of gratuity as a right
 - Undue trust in free providers (e.g. malware behind free software)



TRUSTWORTHINESS

- **End user equipment**, the weakest point
- Public-private partnerships are required for coping with **critical infrastructures** risks, using market incentives for involved agents to bear the cost of trustworthy systems, in particular in security aspects
- Relevance of **certification schemes** (e.g. CC) in critical infrastructures and other elements of business provision
 - Certification schemes and agents need to evolve to cope with the foreseeable needs (time, cost, volume) of this market
- **Audits** to play a major role, e.g. in privacy regulation enforcement
- ITC **systems engineering** offers room for R&D able to cope with reliability & availability requirements yet from design rather than through over allocation of resources (e.g. redundancies) and operational maintenance (e.g. RAMS)
- Industry concentration versus **technological diversity** (i.e. increased security)
- **Open source** to play increasing role

ACTIVITIES IN eSEC



- **eSEC:** Spanish security industry platform
- Recent or foreseen R&D topics on IT Trust & Security :
 - Trustworthy Future Internet (GMV led), affected by
 - IT Services increasing complexity
 - Citizens' data gathering
 - Identity, transparency & accountability
 - Internet jurisdiction & regulations
 - Information minimal disclosure
 - Privacy vs. Responsibility
 - "Patrimonial" /Corporate security:
 - Development and enhancements of technologies and information systems that allow security control over tangible, intangible, information and corporate personnel.
 - Integral dashboards.
 - Support to the development of eDNI applications
 - Evolution of base technology
 - International interoperability
 - Operational environments
 - Certification services
 - Privacy in healthcare sector
 - Identity management and confidential data
 - Secure information storage & exchange
 - Organizational measures
 - Legal issues

OTHER R&D RELATED ACTIVITIES AT GMV

- SERSAF Project (AVANZA): Security in **healthcare** networks of the future. Internet of Things.
- MARTA (CENIT): Security in **vehicular networks**, authentication algorithms in VANETS
- eCID (AVANZA): Application of Common Criteria **certification schemes to critical infrastructure** IT environments
- RED - REaction after Detection (CELTIC): Development of an **Alerts** Correlation Engine and interface console.
- DESEREC (FP6) - **Dependability and Security** by Enhanced Reconfigurability. Events management, advanced rule-based techniques.
- REHABILITA (CENIT): Technologies to support medical Rehabilitation. Handling of **healthcare information**
- CRICTICISM (EC Justice Directorate): Critical ICT Infrastructure **Simulation of Interdependency Models**
 - Mobile devices-based authentication
 - Advanced cryptography for privacy protection
 - Secure computing environments
 - Vulnerability management
 - Fraud detection technologies
 - ...

CONCLUSIONS

- Trust is vital to the future “digital” society
- Future is to be built, it is not determined
- Europe has an opportunity, and an obligation, to shape cyberspaces to conform to their views on rights and values
- The European (not only ICT) industry has its stake in this obligation, and this business opportunity

Thank you

Name: Luis Fernando Alvarez-Gascón

Position: Managing Director

www.gmv.com

UNCLASSIFIED

