



## FIA Prague Trust and Identity in FI sessions

12 May 2009, Prague, CZ

The Trust and Security session was split into 3 slots, with presentations and panel discussions, leaving room for the audience for questions and further considerations. Full agenda and slides are available clicking on the links below in the agenda within Annex 1. The Trust and Identity sessions results were the following:

- **Identity provisioning**, chaired by Jim Clarke. The conclusions are that we see the **emergence of identity and claim platforms**. The concepts of minimal disclosure claims vs (disclosure of full) identity start to become known, with already some interesting applications and trials in pipeline (STORK, Austria, ...). More challenges need to be tackled such as (a) other forms of identity/claim provisioning by and for other id providers, (b) enrich and enhance secure protocols, (c) coexistence of the platforms and how to reconcile them? **The concept of "object-oriented" identity** and context-dependent accountability (e.g. to get redress) also is to be addressed. Last but not least, there is a clear need for **governance** (Who/what is in control?)
- **Trust Platforms** chaired by Volkmar Lotz. **Rich mechanisms increasing trustworthiness start to be available**, with the following challenges (a) dynamic service security based on rich context information; (b) usage control (client-side & server-side models) (c) self-cleaning ID management; (d) trust indicators: metrics and measurements! (e) Interoperability! **User empowerment is essential**, and it needs usable abstractions in order to manage complexity of policies; balancing protection of roles: service consumers vs. service providers (taking into account the "prosumer" role); the user does not see all processes running in the back (SoS). **Regulatory aspects** shows a need for accountability across national borders and the provision of evidence : user to prove a wrong vs service provisioning to prove a right. **Economic aspects are not clear**: where would the compensation for trusted / trust infrastructures come from?
- **Experimental approaches** were chaired by Nick Wainwright along three axes: **Analyse and Measure** (understand how trustworthy future internet is); **Build and Experiment** (provide trust/identity services as enablers in domains of interest) and **Trial and Pilot** (engage lead users (citizens, business) services in application areas of real significance). It gave interesting future work to be explored. Analyse and Measure: How to use the real Internet as our testbed? And Do real users behave as we expect?; Build and Experiment: What enabling capabilities and tools need to be provisioned on which others can build? Trial and Pilot: How to engage real users in pilots? Which areas to focus?

Overall, the audience for the session was around 40 delegates. It attracted the Trust & Security community and a few others from services and experimental facilities. Unfortunately, running in parallel to the MANA and Future Content Networks sessions make it difficult to attract more of the networks audience. We understand that the MANA session (above 80 delegates) at the same time also had discussions about security and threats and it shows that this session was having discussions that the Trust & Security session held on the topic at previous FIA events. In conclusion, the Trust and Identity caretakers felt the session achieved some results and these were presented in more detail in the plenary session (slides available below in Annex 1). However, we feel there is a clear need to engage more with all the research communities around cross domain issues. The caretakers are committed to looking at ways to accomplish this goal including holding other events.

## Annex 1. Agenda and Terms of Reference of Trust and Identity sessions

### Time of sessions

11.30 – 13.30	Future Content Networks (1)	Management & Service Aware Networking Architecture (1)	Trust and Identity in FI (Session 1)
14.30 – 18.30	Future Content Networks (2) Coffee break 16:00–16:15	Management & Service Aware Networking Architecture (2) Coffee break 16:00–16:15	Trust and Identity in FI (Session 2 and Session 3) Coffee break 16:00–16:15

The T&I sessions will start with discussions about the **Trust and Identity Scenarios (see Annex 2)**, with a view to focus on **concrete research challenges** associated with the scenarios. The terms of reference and coverage areas of the 3 sessions will be the following:

**Session 1. ID Provisioning in Service platforms (links with all areas, especially software and services, RWI and content);** Since FIA Madrid focused on ID Management, for FIA Prague, we will instead focus on concrete ID provisioning and dynamic aggregation in service chains. For example, a link to "service description frameworks" and languages, in particular from a naming and a semantic perspective:

- naming: how to extend ID provisioning and monitoring infrastructures to name and identify a whole series of individual (web-based) services and not just users [whether individual or business].
- semantics: how to characterise the "state" of an individual service and the functions it offers [including its security state] so that it can be discovered and composed in future dynamic service execution platforms.

The session will also cover links to industry (eg. Service providers, Telcos) and government ID schemes and platform and methodologies for improving validation of trust and security of SOA's.

**Session 2. Trust Platforms/Tools/Models (links with all cross domain areas);** How to build the platform, examine steps to move forward. Methodologies for accountability, responsibility (usage control/distributed responsibility), consumer protection, regulatory and legal perspectives. Models specifically for Trust and Security including risk and business models;

**Session 3. Experimental and Empirical Approaches (links with testbeds in other areas and with FIRE);** Presentations and discussions about experimental and empirical approaches from the following perspectives: architectural viewpoints, protocols to ensure proper global ID, examine relations with FIRE platforms; possible testbed ideas eg., business over the cloud. It is clear that we need to have an application to keep people interested for testing. We therefore invited people in their presentations ideas to focus on ideas about such interesting applications.

## FIA Prague Trust and Identity Sessions 12-MAY-2009

Slides available by clicking on titles.

<b>Session 1. Identity Provisioning in service platforms (11:30 – 13:30)</b>		
11:30 – 11:40	<a href="#">Introduction to session</a>	Chair – Jim Clarke, Waterford IT
11:40 – 11:55	<a href="#">Keynote 1. Service perspective on FI trust and identity issues</a> Jose Maria Cavanillas, Atos Origin, SPAIN	
11:55 – 12:10	<a href="#">Keynote 2. eGovernment approaches</a> Reinhard Posch, Federal Chancellery AUSTRIA	
12:10 – 12:25	<a href="#">Keynote 2. Validation methodologies</a> Luca Vigano, University of Verona, ITALY	
12:25 – 12:40	<a href="#">Keynote 3. Federated Identities</a> Amardeo Sarma, NEC Labs Europe, GERMANY	
12:40 – 13:20	<b>Interactive Panel session</b> All speakers	Moderated by Michel Riguidel, ENST
13:20 – 13:30	<b>Wrap Up</b>	Chair – Jim Clarke, Waterford IT

<b>Session 2. Trust Platforms (14:30 – 16:00)</b>		
14:30 – 14:40	<a href="#">Introduction to session</a>	Chair – Volkmar Lotz, SAP
14:40 – 14:55	<a href="#">Keynote 1. Dynamic (stateful) service security</a> Mike Surridge, IT Innovation, University of Southampton, UK	
14:55 – 15:10	<a href="#">Keynote 2. Responsibility, accountability and legal aspects</a> Hermann de Meer, Universitaet Passau, GERMANY	
15:10 – 15:25	<a href="#">Keynote 3. Usage control: From distributed systems and information to Clouds</a> Fabio Martinelli, CNR Pisa, ITALY	
15:25 – 15:50	<b>Interactive Panel session</b> All speakers and Luca Vigano, University of Verona, ITALY	Moderated by Volkmar Lotz, SAP
15:50 – 16:00	<b>Wrap Up</b>	Chair – Volkmar Lotz, SAP

### Coffee Break

<b>Session 3. Experimental &amp; Empirical Approaches (16:15 – 18:30)</b>		
16:15 – 16:20	<a href="#">Introduction to session</a>	Chair – Nick Wainwright, HP
16:20 – 16:35	<a href="#">Keynote 1. Perspective from PICOS</a> Pedro Soria-Rodriguez, ATOS Origin, SPAIN	
16:35 – 16:50	<a href="#">Keynote 2. Perspective from Wombat</a> Corrado Leita, Symantec, FRANCE	
16:50 – 17:05	<a href="#">Keynote 3. Experimental and empirical approaches</a> Bernhard Plattner, ETH Zürich, SWITZERLAND	
17:05 – 17:20	<a href="#">Keynote 4. Experimental and empirical approaches</a> Heikki Huomo, Center of Internet Excellence, FINLAND	
17:20 – 18:15	<b>Interactive Panel session</b> All Speakers + Susanna Avéssta (FIREWORKS) (25m)	Moderated by Nick Wainwright, HP
18:15 – 18:30	<a href="#">Wrap Up, including all sessions</a>	All Chairs

## Annex 2

### Trust and Identity Scenarios

1. ICT Infrastructure Scenario: incorporates BUS-VIS and BUS-INC.....	5
2. Service-ecosystem perspective- business moves into the cloud: incorporates BUS-INC ....	6
3. Information perspective Scenario: incorporates BUS-INC and CIT-INC.....	7
4. Client-centric perspective Scenario: incorporates CIT-INC.....	8
5. Threat centric perspective Scenario: incorporates BUS-INC and CIT-INC.....	9

#### Legend for the following tables

1. **[CIT]** One group of scenarios adopting a **citizen-centred** view, presenting (snapshots of) daily activities in living and working in the context of a future Internet enabled society. Such activities could reflect, for example, two complementary dimensions, namely: "I, in my home environment"; and, "I, mobile and *my space* moving with me".

2. **[BUS]** A second group of scenarios adopting a **business-centred** view: what is it for companies or for individuals to make business in the context of future Internet enabled environments?

In addition, each of these two groups of scenarios should be reflecting two different time perspectives:

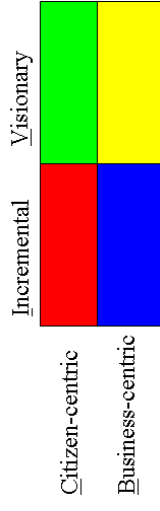
(a) **an incremental perspective** (ie adopting an approach of incremental / evolutionary technology development with regard to today's situation and state of the art)

(b) **a visionary perspective** (ie adopting a thinking that is based on a visionary approach (likely longer term), not necessarily in continuity with regard to the incremental perspective above; such thinking may also integrate a likely disruptive technology evolution potential)

The above are summarised as follows:

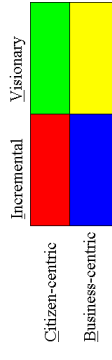
Scenario Nr	Incremental (Evolutionary)	Visionary
<b>[CIT]</b> : Centred on the Citizen (living and working with the F.I.)	<b>[CIT-INC]</b> : adopting an incremental / evolutionary technology development approach	<b>[CIT-VIS]</b> : adopting a thinking based on a visionary approach, integrating also disruptive technology evolution potential
<b>[BUS]</b> : Doing Business by using the F.I.	<b>[BUS-INC]</b> ...	<b>[BUS-VIS]</b> ...

# 1. ICT Infrastructure Scenario: incorporates BUS-VIS and BUS-INC

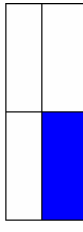


Scenario Description	Functional Description
<p>By 2015, we have reached the tipping point in that more ICT is provisioned as a service in the cloud than is operated by business and enterprise themselves, and the advantages of cost reduction, automation, flexibility, and shift to OpEx is driving the rest in that direction. While not radically different in function from where we are now in 2009, the big shift has been in the provision of ICT to a service model.</p> <p>Pressure on costs, opportunities to outsource, and increased provision of ICT as a service drives ICT users to buy ICT as an operational expense (OpEx) not a capital expense (CapEx). ICT formerly purchased as capital equipment and which was operated by ICT staff employed by corporations becomes an on demand service on the Internet.</p> <p>A server (or multitudes) is purchased or rented as a resource from a service provider. The software formerly purchased as expensive licenses and pricey support contracts is available as a service and paid by the slice. A database (consisting of a few megabytes or a few terabytes) is available from a database service provider. At the same time, computation and storage on demands means that grids go mainstream enabling high-value industry to perform complex analytic computations in every sphere from energy to environment to manufacturing.</p> <p>Whilst it is easy to imagine a successful and thriving ICT services market, some alternative outcomes are also possible. After an initial period of investment and competition a combination of Moore's law and the realisation that computation and storage are an undifferentiated commodity drive prices down in a race to the bottom. Integrated ICT service providers fail to invest to meet the Enterprise grade-SLA's that business customers expect, yet business ICT users under competitive pressure can no longer afford to make the private investments necessary to ensure business ICT continuity, leading to dissatisfaction.</p> <p>Finally, as it is possible that an alternative peer-to-peer market for ICT capacity emerges, mirroring private and semi-private green energy generation, companies can sell-on capacity to third parties on a spot market. This may even extend to private individuals selling on capacity from PC's in their homes.</p>	<p>In a world of shared capacity, we are unable to ensure every user gets 100% <b>availability</b> (no 'brownouts', and no unpredictability). In a global market for service centric ICT, how to ensure interoperability and service level management to meet customer SLA expectations when services are aggregated from different IT and Network service providers?</p> <p>In a world of shared service infrastructure, how to ensure that ICT users get the same levels of confidence in information protection in shared infrastructure that they had when they owned it themselves? This applies to both the trustworthiness of the service provider and the separation of individual customers' information.</p>
<p>From the ICT Infrastructure perspective, the Future Internet has a massive proliferation of nomadic, mobile and wireless devices, together with virtual entities such as virtual private networks, overlay networks and cloud computing. It will no longer be possible to define exact boundaries for their security or to armour-plate every component. Instead, entities will require a capability for managing and negotiating their trust relationships at a more localised level, and helping users make informed decisions about which information, networks, services, systems, organisations and other users with which they interact are trustworthy.</p>	<p>BUS-INC</p> <p>BUS-INC</p> <p>BUS-VIS</p>
<p>Concerns over information security in many industries or countries prevent in using shared services. For instance, a European enterprise is subject to a more complex and restrictive regulatory environment than US or Asian industry and moves slower to take up service oriented IT making Europe less competitive.</p>	<p>BUS-INC</p>

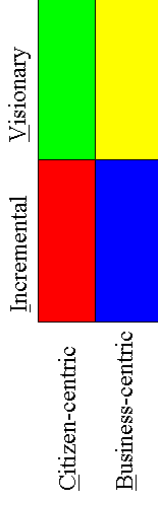
## 2. Service-ecosystem perspective- business moves into the cloud: incorporates BUS-INC



Scenario Description	Functional Description
<p>The trend towards increased integration of business processes from specialized providers available through an Internet of services gathers pace and significantly changes the way business operates. Deeper integration of systems and information between partners accelerates business interaction. The global reach means that a business function can be sourced from anywhere in the world. Global competition opens up interesting new regulatory issues.</p> <ul style="list-style-type: none"> <li>• Services will “become tradable and be composed, offered by different providers’ services, and will be offered, delivered, and executed automatically, and supported with the help of ICT”. It is plausible that events may not go the way that many anticipate, for example: repeated failures in service platforms sensitive information leakage inappropriately between business process partners undermine confidence in deep integration of ICT systems between partners?</li> <li>• A <b>trading scandal</b> emerges involving a cartel of service providers in which a services trading exchange is complicit in sharing information? A single monopoly global trading exchange for services emerges that dominates the way in which services are bought and sold (c.f. Google, Facebook, Amazon?)</li> <li>• Service “<b>Phishing</b>” in the internet of services by ‘rogue’ service providers with the intent of defrauding legitimate businesses. Malicious services exploit their access to information in order to tamper with the business they are integrated with.</li> <li>• Inability of citizens to identify genuine and worthwhile service providers from all the noise (<b>service spam</b>).</li> </ul>	<p>In order to increase trust and confidence levels, research must focus on a number of the key elements necessary for securing the applications and services operating across the future large scale networks and networked systems. These include trust management models handling reputation, recommendation, and history, as well as technical features and their articulation. To ensure a trustworthy <b>Internet of services</b>, the many different virtual entities providing services must be required to adhere to a number of principles:</p> <p><b>Transparency</b> - clear visibility of the events and actions occurring throughout the internet of services with visibility also to appropriate regulatory authorities and maintenance of appropriate records of transactions over time</p> <p><b>Responsibility</b>- the ability to see who or what entity or person is responsible for actions and consequences in the internet of services</p> <p><b>Accountability</b> for actions that are taken with the ability to determine the appropriate relationship between virtual entities and the corresponding legal entities and persons.</p> <p><b>Assurance</b> – the provision of evidence that the service is about to behave as expected and is abiding by the policies and constraints that are imposed on it.</p> <p>Without these principles in place, an Internet of services may encounter significant problems in the future. We should remember that physical entities (<b>Internet of Things</b>) play a part in this Internet of Services, whether gathering information (sensors) or acting on the real world ( e.g. modulating the flow of traffic) and that devices, of which there may be billions, must be accountable ultimately to some person or legal entity.</p>



### 3. Information perspective Scenario: incorporates BUS-INC and CIT-INC



#### Scenario Description

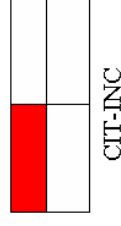
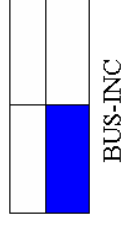
In the 2015 information-centric Future Internet, the opportunity to exploit vast quantities of **information** and results in new information service business that analyse, trade, and deliver insight across the entire gamut of business and personal life. Such comprehensive information gathering facilitates customisation and personalisation of every possible internet service. New intermediaries emerge that trade in and extract new value from this data and information. The information value chain develops in interesting new ways as data gatherers, traders, analysers, users form an ecosystem of information services.

Information is routinely acquired and aggregated in real, including the digital 'trail' left by people, business records of every kind including financial records, transactions, documents, customer information, information captured and managed on our behalf by public sector and quasi public sector organisations such as health care, social services, and tax, user generated content created by and knowingly published by citizens to their own social networks and to the world at large, information 'sensed' from the physical world including security cameras, traffic sensors, cameras, proximity sensors, etc.

Above all, citizens expect to be in control of their digital existence. With that in mind, regulatory authorities expect information providers and users to behave responsibly with clear guidelines on information stewardship. Most of the concerns here come under the area of information stewardship, which will be a significant issue for many aspects of the Future Internet. For example, as information is gathered explicitly (internet of things, future media internet) or implicitly (future networks) about what citizens and business are doing and how they are behaving: Privacy – Appropriate use - User-centricity.

#### Functional Description

Most of the concerns here come under the area of information stewardship, which will be a significant issue for many aspects of the Future Internet. For example, as information is gathered explicitly (internet of things, future media internet) or implicitly (future networks) about what citizens and business are doing and how they are behaving:



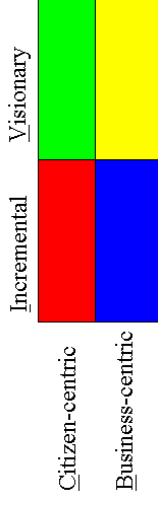
**Privacy** – how to ensure that whilst the 'right' people can get deep insight about individual citizens, the 'wrong' people are not able to see this information.

**Appropriate use** - who are the 'right' and the 'wrong' people and what use can they put information too? While restrictions on information usage can be described today, how can they actually be enforced (and evidence of the enforcement be produced)?

**User-centricity** – how to ensure that information is incorrect, inappropriate, or unjustified, citizens can have it corrected or removed, especially when that spans many different independent information bases.

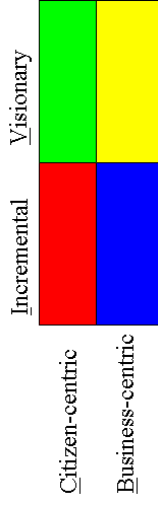
Concerns over information security in many industries or countries prevent in using shared services.


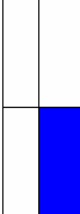
#### 4. Client-centric perspective Scenario: incorporates CIT-INC



Scenario Description	Functional Description																									
<p>By 2015, after years of information breaches, inappropriate uses of personal information by companies, lack of transparency with multi-party services and almost everyone having been effected in some way by identity theft, citizen confidence in others holding their personal information or acting as information mediators on their behalf has reached an all time low.</p> <p>People have turned to what they have, their personal devices, to mediate on their behalf. These devices based on virtualisation technologies to provide separation of concerns, and trusted computing technologies to provide remote attestation and guarantees, allow multiple virtual appliances to safely coexist in one physical form factor. Users have become confident in carrying out online banking in their banking virtual appliance whilst browsing dangerous parts of the Internet in a use-once browsing virtual appliance, knowing full well that spyware and other Trojan software is being downloaded, precisely because their device is keeping these two worlds separate. Because the devices can report back measurements of these virtual appliances in a way that the user cannot corrupt, service providers, such as banks, have confidence that software hasn't been tampered with. For such important services as banking, online voting, or payment, responsibility for managing appliance security, and consequently liability, has shifted from the user to the service provider.</p> <p>Privacy enhancement is provided by the device taking the responsibility to automatically keep the user anonymous unless instructed otherwise, new email addresses being established for each new service subscribed to. In fact a whole new business has sprung up providing templates and avatars allowing users to be whatever they want to be. In contrast to the information-centric and service-ecosystem perspectives, individuals now leave far less of a digital trail and it is service providers that have little confidence in the accuracy of the information they receive. Genuine information is something that users reveal only to service providers that have earned their trust.</p> <p>Businesses no longer buy clients relying on their employees to give up control of a virtual business "desktop" to corporate IT. And the flexibility to create new virtual appliances allows businesses the same safety that consumers enjoy to try new service offerings without putting what they already have at risk.</p> <p>Federation of virtual appliances across multiple devices allows individuals seamless access to services. This federation also allows information sharing across families, extended families, communities small and large, and even nation states; social networking has taken advantage of this ability to form agile, light weight closed communities.</p>	<p><b>Trust security and privacy issues across domains include:</b></p> <p>Virtualisation to provide separation of concerns, and trusted computing technologies to provide remote attestation and guarantees, allow multiple virtual appliances to safely coexist in one physical form factor.</p> <p>Privacy enhancement is provided by the device taking the responsibility to automatically keep the user anonymous unless instructed otherwise.</p> <p>Genuine information is something that users reveal only to service providers that have earned their trust.</p> <p>Federating across multiple devices allows individuals seamless access to services. Information sharing across families, extended families, communities small and large, and even nation states; social networking has taken advantage of this ability to form agile, light weight closed communities.</p>	<table border="1"> <tr> <td style="background-color: red;"></td> <td></td> <td>CIT-INC</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table> <table border="1"> <tr> <td style="background-color: red;"></td> <td></td> <td>CIT-INC</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table> <table border="1"> <tr> <td style="background-color: red;"></td> <td></td> <td>CIT-INC</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table> <table border="1"> <tr> <td style="background-color: red;"></td> <td></td> <td>CIT-INC</td> </tr> <tr> <td></td> <td></td> <td></td> </tr> </table>			CIT-INC						CIT-INC						CIT-INC						CIT-INC			
		CIT-INC																								
		CIT-INC																								
		CIT-INC																								
		CIT-INC																								

## 5. Threat centric perspective Scenario: incorporates BUS-INC and CIT-INC



Scenario Description	Functional Description
<p>By 2015, our total dependence on ICT has made the online world the number one area of activity for organised crime, state sponsored espionage and activist groups.</p> <p>Many activist groups have moved beyond the world of blogs and viral marketing to activities they regard as online civil disobedience but others regard as cyber-terrorism. Unions no longer picket physically but rely on new social networking technologies and forms of online advertising to reach much greater and targeted audiences. Each of the other perspectives above also allows for extremes of behaviour that many find unacceptable. Citizens are divided in their views, with many individuals feeling a mix of being liberated and threatened.</p> <p>Technologies to protect citizens and businesses, together with the complexities and cross border nature of the Future Internet, make it easy for criminals to hide their activities. Most citizens have become increasingly frightened by cyber-crime and perhaps the greatest threat to the Future Internet has become the possibility of politicians seeking to re-establish safer participation by over regulation and control. But politicians have also become aware that many of the measures that some would like to see are potentially double edged. Demands that all new software should be produced to high levels of security and privacy engineering threaten to slow the introduction of new services or make them uneconomic in comparison to cheaper services from other countries. Demands for tougher penalties on hackers and demands that universities should be prevented from teaching hacking skills, particularly when other nation states actively train their students, could mean that Europe doesn't have the skills base necessary in coping with a future cyber-war.</p> <p>New technologies continue to be created and used, old technologies are being used in new ways, combined with the talent available to organised crime, by 2015 new vulnerabilities are being discovered, exploited, bought, sold and used at a rate that police forces and intelligence agencies struggle to keep up with. Many countries have all but given up trying.</p>	<p><b>Trust security and privacy issues across domains include:</b></p> <p>Future-proofing against known and currently unknown threats and vulnerabilities, assessing and managing risks, assessing and managing liabilities, accountability for actions and decisions that are under obligations, managing information rights, managing oversight and control, including at a state level, security-aware languages, automated security configuration driven by end-user's needs, evolutionary and predictive threat models, self-organising and self-healing security mechanisms , ...</p> <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  <p>CIT-INC</p> </div> <div style="text-align: center;">  <p>BUS-INC</p> </div> </div>