IJPIS

A PHILOSOPHY OF PUBLIC SERVICE

- ARCHITECTURAL PRINCIPLES FOR DIGITAL DEMOCRACY

PHILIPPE CHARAS
Minerva Insight
philippe.charas@3mail.se

PER JOHANNISSON
Swedish Defence Material Administration
pelle.johannisson@telia.com

OLOV ÖSTBERG
Swedish Administrative Development Agency
olov.ostberg@verva.se

Abstract

This paper sets down architectural principles as seen from the perspective of a Public Service being part of a constitutional framework and aims at defining Public Service from the viewpoint of IT Architecture. The key features are the concepts of Policy and Policy Enforcement, which are integral parts of the Architecture while also introducing a hitherto missing component, namely the Legal Dimension.

Keywords: IT architecture, public service, principles, e-Government

1. Scope

The Scope of this document is twofold:

A) To set down architectural principles as seen from the perspective of a Public Service being part of a constitutional framework, and
B) To define Public Service from the viewpoint of IT Architecture.

There are some problems associated with Public Service inheriting an unmodified Enterprise Architecture from incumbent business. To what extent can Public Service be seen as an Enterprise without colliding with the constitutional framework in which it should be embedded?

To what extent can a modern democracy maintain its credibility towards its voting constituency if it is perceived as an Enterprise, indistinguishable from other Enterprises?

2. Architecture

In his famous treatise On War, Carl von Clausewitz sees War as a continuation of Politics by other means, and accordingly feels that war can never successfully be

conducted in its own right without the support of the people[1]. Similarly, processes which have been enabled by an architecture must also be seen as the continuation of politics by technical means, and as with the war scenario, cannot be implemented without due consideration to public sentiment.

Architecture is always subject to a main requirement, an *inherent intent*, governed by either a business model or a legally driven public policy. On top of this we have secondary requirements, financial, time-related and aesthetic, etc., but the main *requirement with its inherent intent is and remains the cornerstone defining the structure of the architecture.*

Secondary requirements, although important, because they govern issues such as flexibility, cost, and aesthetics, must not be confused with the main requirement which is the architecture's suitability with respect to the *inherent intent* of a particular business model or Public Policy.

This fundamental separation between *intent* (strategy) and *physical implementation* (tactics) is fundamental in creating the architecture, since it goes well beyond short term implementation issues, such as "standards politics" which often plagues so many implementation activities, guaranteeing a longer term survival of the structure itself.

3. Doctrine

A democracy's *inherent intent*[2] manifested by its societal processes is found in the doctrine defining the main rules governing its Information's Architecture.
The doctrine defines the main goal and ethics[3] governing the architecture to be implemented[4].

In our case, the doctrine must follow the rulings of a constitutional democracy. At this level no conflict between the architectural doctrine and the inherent intent of public policies can be permitted since the public e-space exists (??) under the main requirement, namely to satisfy the inherent intent of the public policies. The inherent intent of democracy is the implementation of laws passed by a democratically elected legislative body at the national or EU level. *The executive branch of government and government agencies are responsible only for the execution of laws passed by a democratically elected legislative body*.

Independent auditors and an independent judiciary are responsible for monitoring the execution of laws passed by the democratically elected legislative body. This division between *executive, legislative and judiciary* powers is common in the western world and follows the principles of Montesquieu, which is also at the core of the doctrine for Informational Architecture in the Public e-space[5].

---

[1] In this way Clausewitz unknowingly, but cleverly predicted the collapse of the Romanovs, the Habsburg Empire and the demise of the Prussian Kaiser Wilhelm II as the 1st World War committed the masses.

[2] Elliott Jaques' pioneering work in organisational theory and the behaviour of living organisms is based on a number of fundamental concepts. One of these is the concept of"*inherent intent"*; an organism's organic and architecturally based endeavour to satisfy its inherent intent. The Life and Behaviour of Living Organisms, A General Theory, Chapter 8, Elliott Jaques, Praeger, Westport Conn. ISBN 0-275—97501-0

[3] Ethos, Logos and Pathos are the three fundamentals pillars of the architecture which are defined by the doctrine that governing the EA

[4] A doctrine in the supplement is written for the Swedish Administrative Development Agency.

[5] By Public e-Space is meant the domain within cyberspace occupied by public electronic and informational services.

Secondary requirements often pertain to the efficient and fair use of resources. It will be shown at a later stage that the executive branch of government need not own the resources, as it is sufficient that the government agency in question controls enablers for accessibility, trust uniformity and customer satisfaction, and monitors that requirements for accessibility, trust, uniformity, quality and customer satisfaction are fulfilled.

Other secondary requirements are those pertaining to the formation of federations of government agencies. This is a requirement governed by the need for updating, and continuous restructuring, particularly in emergency situations where authorities may be required to cooperate on a more or less ad-hoc basis, dictated by unforeseen circumstances.

4. Architectural Principles/Main Requirements

Architectural principles demand a full separation between the parts of the architecture that relate to the tripartite-constitutional subdivision into the legislative, executive and judiciary domains. The functional subdivision as defined by the architecture must provide well defined interfaces uniquely defining agency roles, protecting civil rights and the citizens right to interactive services; abiding to laws passed by the legislative body.

4.1. Local Policy Enforcement[6]

Laws passed by the legislative body are converted to Digital Instruments → *Policies*. Policies can be seen as certificates, and instead of certifying a person they certify a *right*. The combined digital entity Certificate and Policy define a specific individual's right and can enable the execution of a service by a local authority or government agency anywhere in the public e-space. This is called Local Policy Enforcement. The connotation *Policy* must, in this context, be seen as a well adopted technical term invoking loosely coupled services between technical systems and should not be confused with policy as a political instrument, although they are related.

4.2. The Concept of *Legalities* - Reflecting Legislative Power in the Public e-space

An individual's national identifier, for example SE-ID and his/her Policies, meaning contractual obligations, expressed in a data format, are called *Legalities*. These can be stored locally in a secure portable environment or centrally in a database, or, quite probably, in both depending on the security classification associated with a particular policy. Severe restriction can be applied to some policies and they may only be valid for a short period of time; the remit for others can be extensive and they may be valid over a very long time period. Policies are defined using a consistent syntax and are guaranteed by a Central Policy Authority (CPA), much like a Certificate Authority (CA). These legalities can be communicated securely to and be read by the

[6] The concept of Local Policy Enforcement, can be seen as an extension of IETF´s (Internet Engineering Taskforce) terminology for AAA baserad Policy Enforcement. http://www3.ietf.org/proceedings/01mar/I-D/policy-terminology-02.txt,
US Patent 7,054,843, and 6,880,009 concerning Local Policy Enforcement in heterogeneous environments.

surrounding public e-service domain, using a suitable interface intended for secure communication of legal rights[7].

In this way legalities provide *a communicable image of an individual's legal rights in the e-service space*, reflecting his or her rights as provided by a democratically elected legal body. Just as drivers' licences and passports imply certain rights, so do policies. Just as banknotes provide legal tender if presented for a service, so policies provide legal tender and are linked to a particular individual when presented in the form of legalities.

4.3. The Concept of *Legal Processes*

Legalities can be used for *identification* (Authentication), or provide *access* to (Authorization), or have a Policy or Certificate *validated* by an external third party (Validation) or provide *accounting or auditing* information (Accounting). Normally these legal processes or events are given the acronym AAA (Authentication, Authorization, Accounting). As the complexity of the e -service space evolves more and more legal processes can be defined. It is conceivable that as time goes by a whole set of hierarchically related legal e-processes will evolve and be standardised within one and the same syntax.

The important aspects are that; they are *independent* of both:

- The legalities that are used as drivers for the legal processes

as well as

- The resources that will be subjected to the legal processes interfaced by the service

For example Authentication of an individual person is independent of the Service to be provided to that individual and additionally Authorization, Validation, Auditing and Accounting are performed independently of the service or resource in question.

We must again remind ourselves that: Legal Processes are independent of resources, Services, Service Providers - and Government Agencies and that they span society as a whole and are common to the whole of public e-space.

Adherence to this statement will mean gigantic savings for everybody, in standardisation, in implementation, and in support etc. as well as opening up the possibility for trans-national, trans-European and global federations at the public e-services level. It is of such immense importance that it should become a prioritized project under the supervision of the EU Commission.

Today, the Euro is a reality; bookkeeping and auditing principles are well established across nation boundaries so why should all resource owners be given the right to define their own legal processes within the e-services domain, carving out a monopoly for themselves and owning the customer? Many present day government agencies still maintain a feudal attitude towards the citizens they are supposed to serve. *The three freedoms of persons, capital, goods and services also imply borderless legal processes in public e-space.*

The executions of legal processes belong to the executive branch of government and can be seen as their core business. They are, and must be, seen as completely separated from service production which in turn can be delegated to entrepreneurs providing they satisfy public e-service standards.

[7] Within the federation" Liberty Alliance" an **XML** based SAML **S**ecurity **A**ssertion **M**arkup **L**anguage is used for communicating digital rights between players within the same federation.

Maintaining user interfaces and *the execution of legal processes*, driven by legalities from the legislative process that *guarantees service availability, trust, uniformity and customer satisfaction* are the main tasks of the executive branch, and *cannot be* delegated without the executive government agency relinquishing its main task and losing its right to exist.

4.4. Managing Resources and Capabilities

Resources are subject to operating under legal processes, and are operated in order to provide a service to the citizen or consumer. The architecture is indifferent to the ownership of the resources, and does not care whether these are owned by a government agency, a private company or a non governmental organisation. The enactment of legal processes on the resources is uniform[8] across the whole of the e-services space.

This opens up many types of federations at the resource level, such as;

Government agency ⊗ Government agency;
Government agency ⊗ Private entrepreneur; or
Government agency ⊗ Government agency ⊗ Private entrepreneur.

The only requirement is that one agency takes the lead, and acts as a primary representative of the federation which, as shown above, may include resources and capabilities from both the public and private sectors inside the same country and abroad which have common interfaces to legal processes in similar proxies[9].

At the governmental agency level we now see a clear separation between, on the one side, the legal processes and on the other side resources for the implementation of services; a fundamental separation of roles that must occur within government agencies.

4.5. Architectural Principles, Organisational Meta Structure

Figure 1 below presents a three-layered view consisting of Legalities, Legal Processes and Resources enabling Local Policy Enforcement across a wide public e-services space. These are, as stated previously, three logically, completely separated informational and legal entities reflecting the tripartite separation as seen in modern democracies. Focus here must also be on the interfaces between the three entities, because these interfaces essentially define the scope of government agencies as seen from the informational perspective. The interfaces essentially and brutally define what is or not, a government agency. Whether it exists under the legislative or executive branches of government or whether it is merely a resource to be procured on the open market, in essence and is, by definition, not a government agency at all. In defining Information Architecture one must be honest. Interfaces between entities cannot be manipulated or be subject to politicking and must follow the inherent intent of a democratic society.

[8] Uniform in this case means that resources are subject to the same interfaces to legal processes.
[9] The GSM network infrastructure is a global federation using common legal processes, and common legalities (SIM). The early adopters of GSM ETSI as well as the main industrial players Ericsson and Nokia were too focused on Wireless Technology and never realized the far reaching architectural ramifications of GSM

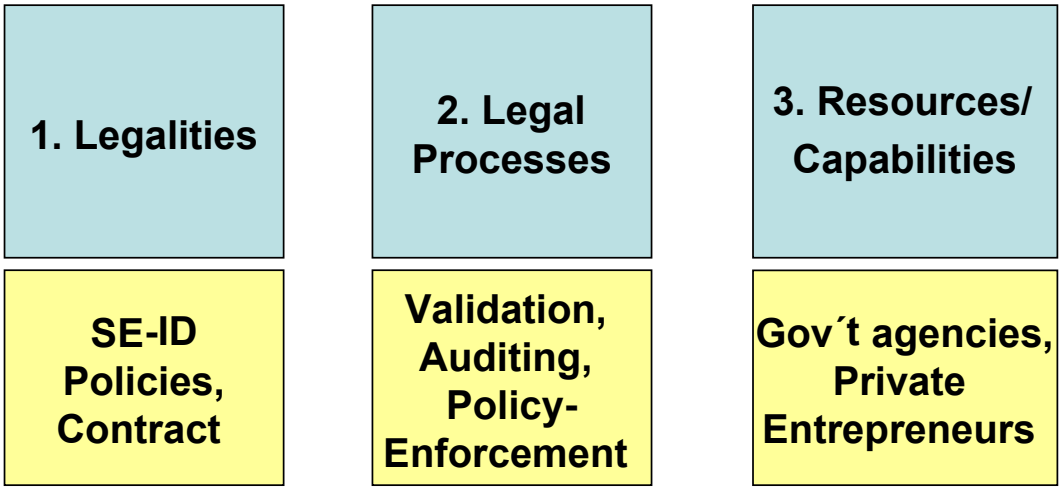

Figure 1. Architectural principles in three dimensions.

Layer 1. Legalities. **Hinc Robur et Securitas[10]. Here is Strength and Security**. Legalities and data carrying contract related information[11] must satisfy standards and be accessible within the whole public e-services space governed by a policy framework. This layer has a ***brand carrying capacity*** and represents trust, security, and equality, yes equal and fair treatment across the whole e-services space for all citizens. *Legalities are the prime representative and enabler of the legislative branch* and therefore embody in their syntax of policies the inherent intent of democracy. This layer is a prerequisite for all enabling of e-services in the public domain and governs all service provisioning from a legal perspective.

National-ID , policies and contracts are stored and managed centrally by a Central Policy Agency CPA. This CPA can be seen as an extension of the national bank and just as currency is basically a pan-European issue, the standardisation of policy syntax and policies should be a pan-European issue and be part of the European bank. The storage and management of policies governing the citizens' rights in the e-services space is an issue for the nation-state.

Layer 2. Legal Processes. **Pacta sunt servanda[12].** Agreements shall be honoured; this is the central task of the executive branch of government, honouring agreements made within the democratic system.

Legal processes provide accessibility to resources; in doing so a number of legal processes can be activated. It could be Authentication, identifying a user, Validation checking with the CPA the validity of a particular identity or policy in order to invoke the government services. In addition it could be authorizing the use of a particular resource in the private or public domain, benefiting the citizen according to a set of rights defined by the legislative body of government stored and managed separately from government agencies belonging to the executive branch.

The executive branch operates between the interfaces as defined between legalities and the resources or capabilities.

All agencies belonging to the executive branch ***share a common set of legal processes***, and in this way can act either on their own or work together in federations

[10] This was the former motto of the Riksbank, The Swedish National Bank.
[11] that is regulating the relationship between the citizen and the service provider
[12] ***Pacta sunt servanda*** in latin "agreements must be respected"

within the same country or across national boundaries. This part of the agency is logically separated from that part which belongs to Layer 3 Resources and Capabilities; however this is only from the logical perspective. When implementing a complete service it is often suitable to co-locate the execution of legal processes and resources in the same physical premises.

Layer 3. Resources and Capabilities.
Although Layers 2 and 3 participate together to form a service, it is as said previously, important to separate these layers. Technology tends to evolve much faster than the legal processes of society. The separation thus guarantees that the architecture can easily cope with the advancement of science and the incorporation of new and previously un-thought of resources. Also, legal processes can be added as society evolves without necessarily having to involve resource owners or modify the resources as such, except for the interfaces to the legal processes.

5. Architectural Principles, Final Comments and Considerations

This three-layered architecture is a logical consequence of the current on-going layering of systems architecture, manifesting the transformation from a vertically integrated nation-state to an open service globally oriented society, based on horisontalisation and economy of scale. Current SOAs (Service Oriented Architecture) as defined by OASIS are a way of defining a system of systems and does not contradict a separate legal domain consisting of legalities and legal processes. The above three-layered model requires well defined interfaces between levels 1 → 2 and levels 2 → 3.

In the case of 1 → 2 we see an interface able to securely communicate contract related data such as Identities and Policies, necessary for the execution of policy driven processes which we have termed legal processes.

In the case of 2 → 3 we have an interface which is capable of making resources available for a particular policy driven application, such as producing a passport, driving license or booking a health examination as part of the National Health Service (NHS). In this case patient data, identities and policies are stored and placed at the disposal of the NHS which are utilised to provide equal and fair access to resources available to the health care federation.

Our discussion, to date, has been focusing mainly on fundamental issues related to architecture and inter-organisational subdivision of responsibilities; how we feel they should be positioned from a legal perspective guaranteeing citizen rights in a democracy. We have not discussed requirements that need to be otherwise imposed on an SOA defined by a loosely coupled federation of rather independent government agencies, such as is the case in Sweden or centrally and more strictly controlled government agencies such as in some European countries with other traditions of government since this is already underway. What is clear however is that architecture that focuses solely on ownership and resource management, lacks a legal dimension, and a control plane emanating from the individual civic rights as defined by a democratically elected legislative body, will place power solely in the hands of the resource owners; this forms the basis for a bureaucracy that sooner or later will be plagued by human weaknesses, manifesting poor accessibility, lack of trust, inequality

and customer dissatisfaction[13]. The question we must ask is for whom are we building an informational architecture; for the enterprise or for the citizen? Can the nation state as it has evolved during the 20th Century be seen as an enterprise at all and be a platform on which we can build equitable e processes? Is the control of resources or the control of rights the sine qua non of a service oriented democracy or federation of democracies such as the European Union?

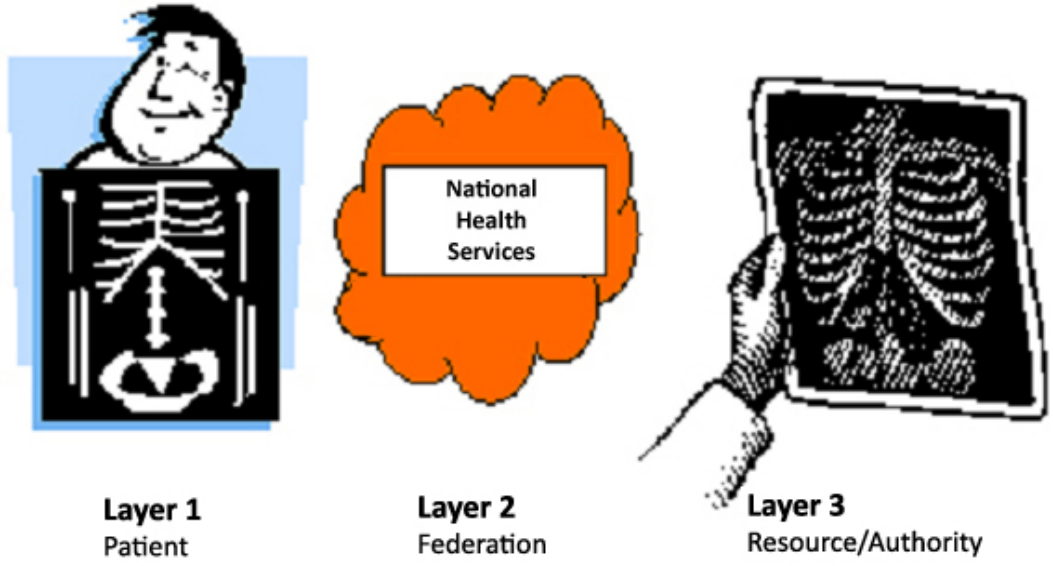

Figure 2. Architectural principles Applied to the Swedish National Health Service.

6. Federated Services Vision

It is not the intent of this paper to be very specific with reference to implementation, since this can be achieved in a number of ways. None of the aforesaid however is really in conflict with the OASIS concept of a Service Oriented Architecture and if we base our discussion on the three-layered approach discussed previously, we can conceive of a number of entities.

1. Citizen terminal, hardware, TV, mobile terminal, personal Computer or software only, enabling secure access via a VPN tunnel to a secure e-Government Proxy managing legal processes.
2. A secure Government Proxy server or cluster of servers providing access to a single or federation of Government Agencies that provide services to the citizen along lines legislated by the legislative branch of government.
3. An Independent Central Policy Server or cluster of servers under the auspices of a Central Policy Authority, managing Identities, Rights, Obligations and Shared Secrets, answering questions upon request from Government Agencies and federations thereof providing and guaranteeing trust.

[13] The Swedish national Health system that despite large investments is an example of a resource instead of citizen rights driven structure, plagued by inaccessibility and inconsistent quality.

4. An SOA enabling service provision to fixed and mobile users, via many different media, IP, Mobile, Mobile IP, and Broadcast. Service provisioning is agnostic to the type of service delivery.

Figure 3 below indicates the Infrastructure Vision with some important qualifiers. Just as a nation-state owns, distributes and controls citizen and geographic identifiers such as IDs, street numbering, etc., in order to be able to govern, so it is logical that the nation-state also has control over Numbers Naming and Addressing of its e-government Intranet and does not relinquish this control to ICANN (International Consortium of Numbers Naming and Addressing). For this reason tunnelling between the Citizen Terminal and e-government secure proxy becomes mandatory if networks are to be shared and e-government services are to be generally accessible.
Policy information, although managed in a Central Policy Server, can still be distributed in secure (hardware or software based) policy repositories in user terminals.

IP based protocols allow multiple forms of service distribution and service provisioning.

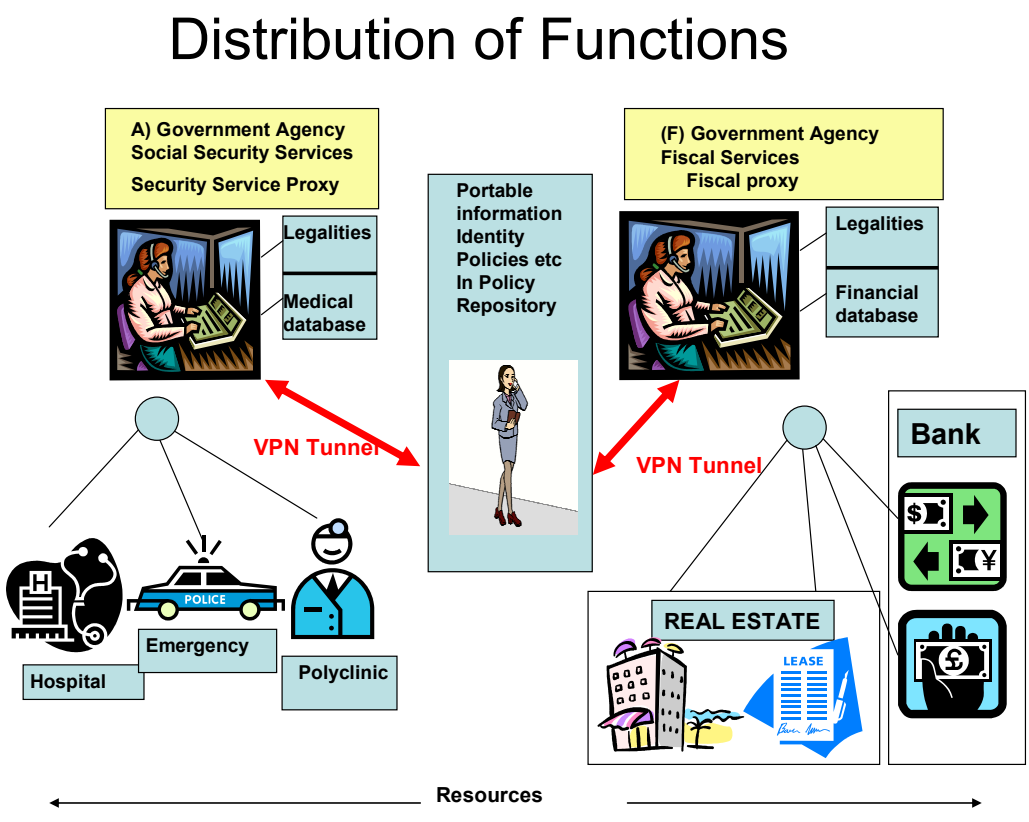

Figure 3. Generic physical application of the architecture in the public and private domains. The three layers described in section 4.5 are discernible.

In Figure 3 above, the three layers described previously in § 4.5 of this paper can be identified.

Layer 1. In the middle, top centre is the citizen, describes as a "roaming database" carrying legalities (identifiers and policies) in a policy repository, mirroring part of the policies stored in the CPA. These can be communicated through a VPN tunnel, marked in red, to layer 2 using a well standardized interface for communicating legalities, i.e. rights obligations and shared secrets.

Layer 2. Top left and right, can be seen as Government Agencies, in yellow, in this case exemplified by a Fiscal Agency (F) and a Health Care Agency (A) that operate legal processes from a Secure Proxy, terminating the VPN tunnel between itself and the Citizen. Here designated as Security Service Centre Proxy and Fiscal Proxy.

Layer 3. This layer can be seen at the bottom of the picture. Resources and capabilities, in this case health care and financial resources, supporting the fulfilment of rights as in the case of health care services and obligations as in the case of the fiscal services, based on legalities. In both cases, the Government Agencies, here manifested by the Secure Proxies have access to the resources and capabilities; in the case of (H) to make available resources to the citizen, and in the case of (F) to verify fiscal information that the citizen has released to the fiscal agency by virtue of a suitable policy.

7. Supplement - An Example of an e-Government Doctrine

1. The doctrine presupposes a federated architecture enabling/supporting a public service offering which places the customer in focus and contains the following ***four*** underlying attributes ***availability, trust, uniformity and customer satisfaction*** and are subject to the democratic society's, principles and legislation.
2. The doctrine supports the citizen and guarantees his/her information integrity through his/her life cycle.
3. Government agencies are responsible for the service offering in cooperation with other agencies and in accordance with the constitution and other principles and rulings.
4. Government agencies act in a loose federation which means that they act under common terms of reference, a common code of conduct and common interface principles whose goal it is *to enable trust and customer satisfaction under a common national brand.*
5. The federated architecture, a common federated SOA provides information in dedicated interactive channels to citizens and legal entities.
6. The federated architecture provides information based on data that is the property of the citizen and whose integrity is guaranteed by the state. This data is available to all government agencies on a need to know basis only. This must satisfy the prerequisites of 2 above, trustingly uniformly etc...
7. The federated architecture enables a structured selection of public e-services.
8. Quality Assurance. The federated architecture provides via § 3 'benchmarking' between government agencies due to standardised and common practices for quality assessment, assessment of customer satisfaction, and quality reporting. Quantitative and Qualitative measurements are performed, both internally between agencies as well as towards the customer. Quantitatively, with zero errors being the ultimate goal and qualitatively, to minimise capital tied up in erroneous service

processes, resulting in improved throughput, improved productivity and customer satisfaction. .

9. Continuous improvement. VERVA, The Swedish Administrative Development Agency, acts as a quality coordinator and as a quality agent improving and updating the federative architecture, reporting monitoring and reporting quality to the Ministry of Finance. The national auditing office performs quality auditing and reports to the parliament. All government agencies identify the individual's responsibility for quality in their respective organisations, reporting to VERVA, The Swedish Administrative Development Agency.
10. The federated architecture is developed and updated to satisfy EU requirements.

References

von Clausewitz, C. (1976/1984). *On War*, Howard, M. and Paret, P. (eds.), Princeton University Press.

Jaques, E. (2002). *The Life and Behaviour of Living Organisms: A General Theory*, Praeger, Westport Conn.