Distributed Interoperability and Electronic Signature

Red GEALC

EL SALVADOR
Grande como su gente

SECRETARÍA TÉCNICA
Y DE PLANIFICACIÓN
DE LA PRESIDENCIA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

Before we begin

Service Oriented Architecture and its many interpretations

SOA, What do we mean?

- Initial vision for SOA(2001) was centered around processes: governance, mapping, functional decomposition[1].

  SOAP, OASIS WS-*, BPM/Enterprise Service Bus, etc.

- These days SOA is more centered around the end users and therefore applies more flexible standards.

  Containers, APIs/Web Services, IC –DevOps

  https://www.programmableweb.com/category/all/apis

- SOA is just an idea, it has no concrete meaning. The main architecture principles and components now have a life of their own[2].

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

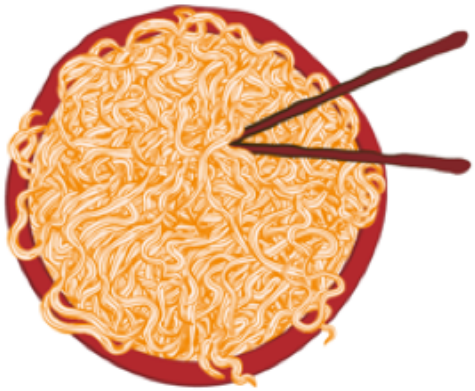
1- American Quality and Productivity Center, Plantilla de Classification de Procesos, https://www.apqc.org/pcf
2- Service Oriented Ambiguity
https://www.martinfowler.com/bliki/ServiceOrientedAmbiguity.html

The evolution SOA

Dependencies from a developer's perspective

1990s and earlier

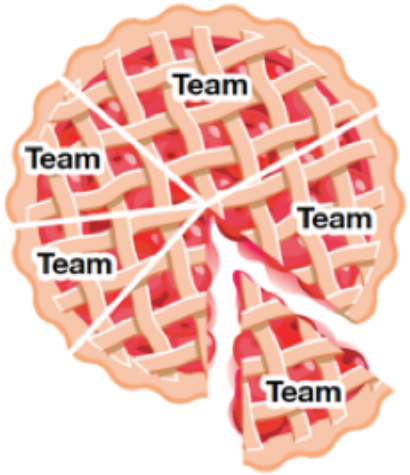
Pre-SOA (monolithic)
Tight coupling



For a monolith to change, all must agree on each change. Each change has unanticipated effects requiring careful testing beforehand.

2000s

Traditional SOA
Looser coupling



Elements in SOA are developed more autonomously but must be coordinated with others to fit into the overall design.

2010s

Microservices
Decoupled

Developers can create and activate new microservices without prior coordination with others. Their adherence to MSA principles makes continuous delivery of new or modified services possible.

GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

PWC, Technology Forecast: Rethinking integration, Issue 1, 2014.

SOA: What are countries doing?

- Several countries have implemented an Enterprise Service Bus (Uruguay, Chile, Peru, Ecuador, Colombia, Costa Rica, Venezuela). This model requires messages to use the ESB as an intermediary.

- Adoption by agencies is difficult. Today, people are connecting services without a middle man, we don't like intermediaries.

- If we are starting from scratch we can learn from our neighbor's experience. That is a big advantage

Context

Basis for the creation of connected government services

Government Services

What do we have:

Slow and complicated government services

Disconnected data spread out across government

Services designed without the user's input

What do we want:

Fast and efficient government services

Data that is shared and connected across government

Services designed with the user

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Where do we start?

Processes:

We need to understand our current back-office processes in order to improve them. This includes reviewing/creating guidelines and training people.

Regulations:

We need to understand the legal barriers. Can we change them? We also need take advantage of enabling regulations, e.g: Electronic Signature Law.

Electronic Signature: Plain vs Qualified*

Plain ES	Qualified ES
Simple PKI tree	Multi level PKI tree
Owner alone (government office) is responsible for its security	Is a matter of national security
Manageable cots	High implementation costs, high barriers for businesses
Registration and issuance of certificates managed in house.	There are mandatory national protocols for registration and issuance of certificates;

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

*El Salvador's Law (2016) recognizes both plain and qualified Electronic Signatures.

When do I use Plain ES?

El Salvador's Electronic Signature Law says:

- Art. 29.- Government authorities and public employees who deliver public services, within their jurisdiction, MAY sign using plain electronic signature.

- Art. 33.- Government offices, MUST communicate electronically using plain electronic signature. (e.g. SMTP,VPN/TLS –Web Services)

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Using X-Road

How are we using X-Road to connect government data in El Salvador

Distributed Interoperability

Estonia was the first country to implement this concept through their X-Road platform in 2001.

- At the heart of X-Road lives a PKI that offers trust services to all the components and services.
- It uses electronic signature to build and maintain an immutable, distributed ledger (prior to Blockchain in 2008)
- Costs and coordination efforts are significantly less than those of a centralized platform.

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

4- Gestión de Acceso https://oauth.net/2/, Seguridad https://jwt.io
5- https://getkong.org/, https://apigee.com/about/cp/open-source-api-management

Why X-Road?

There are many tools[5] to manage services and APIs. However:

- X-Road offers a centralized catalog of published services while leaving access management to the owner agency.
- Complies with the EU security standard for electronic transactions eIDAS
- Creates VPN/TLS tunnels automatically between each client and service owner, eliminates costs of leased lines.
- Enables data exchange between countries using separate federated x-road installations.

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

4- Gestión de Acceso https://oauth.net/2/, Seguridad https://jwt.io
5- https://getkong.org/, https://apigee.com/about/cp/open-source-api-management

Why X-Road?

Because we have an Electronic Signature Law that says we can use (plain/free) Electronic Signature certificates to secure and protect the exchange of data across government agencies; which is exactly what X-Road does.

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

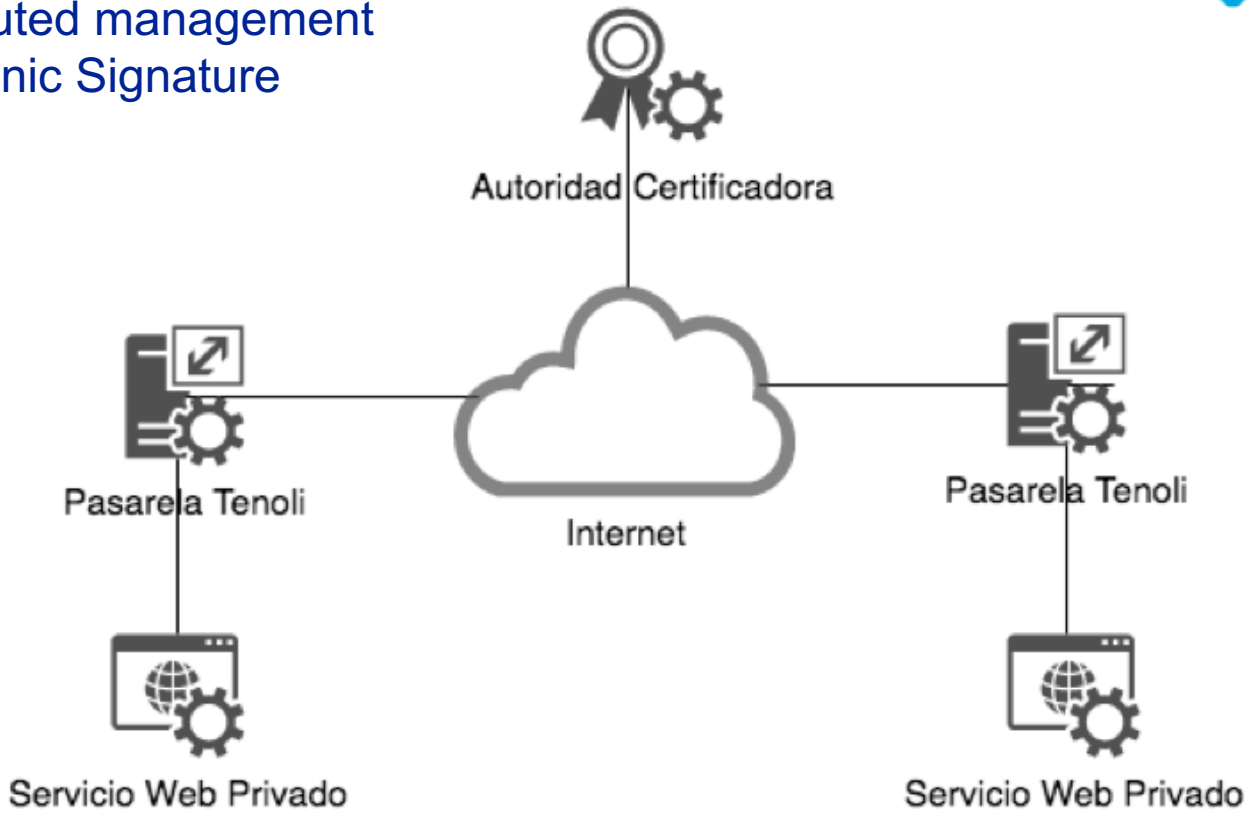
X-Road Salvadoreño

- Management web interface translated into Spanish
- Source code modified to use a local Certification Authority (C=SV,..) currently managed by the EGov office.
- Running in live since Dec. 2016, connecting six government agencies: ISSS, CNR, RNPN, MINSAL, MINED,DIGESTYC
- Available to handle both REST/JSON and SOAP/XML message services using a programming language of your choice.
- We named it ‘Tenoli’ (Nahuatl for bridge)

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Basic Ideas:

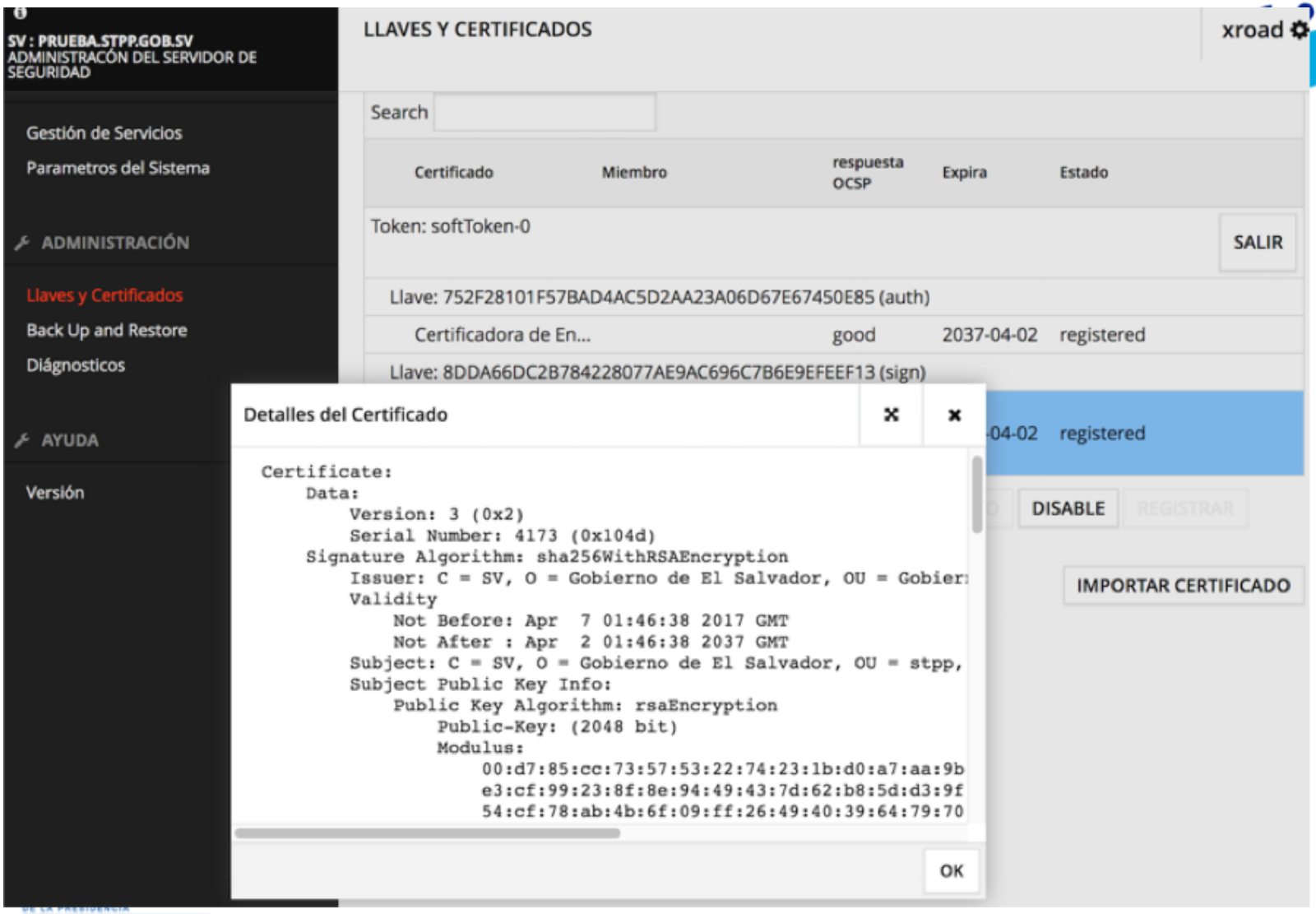
- Interoperability
- Distributed management
- Electronic Signature



Screenshots

- Management UI
- Sample message payloads
- Sample access record
- Tenoli's webpage (training y trainign materials)

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER



GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

```
<soapenv:Envelope
xmlns:soapenv=http://schemas.xmlsoap.org/soap/envelope/
 xmlns:xrd=http://x-road.eu/xsd/xroad.xsd
 xmlns:id="http://x-road.eu/xsd/identifiers">
<soapenv:Header>
   <xrd:client id:objectType="SUBSYSTEM">
         <id:xRoadInstance>SV</id:xRoadInstance>
         <id:memberClass>GOB</id:memberClass>
        <id:memberCode>1001</id:memberCode>
         <id:subsystemCode>consulta-cun</id:subsystemCode>
     </xrd:client>
 <xrd:service id:objectType="SERVICE">
       <id:xRoadInstance>SV</id:xRoadInstance>
     <id:memberClass>GOB</id:memberClass>
      <id:memberCode>3002</id:memberCode>
     <id:subsystemCode>nacidosvivos</id:subsystemCode>
      <id:serviceCode>getNacidosVivos</id:serviceCode>
     <id:serviceVersion>v1</id:serviceVersion>
 </xrd:service>
     <xrd:userId>SV982343432</xrd:userId>
    <xrd:id>0ba036ea-d612-4e74-bf73-59a6f15627c8</xrd:id>
                <xrd:protocolVersion>4.0</xrd:protocolVersion>
 </soapenv:Header>
   <soapenv:Body>
      <prod:getNacidosVivos xmlns:prod="http://api.minsal.gob.sv/producer">
        <prod:request>
                    <prod:fecha_registro>2017-02-01</prod:fecha_registro>
        </prod:request>
     </prod:getNacidosVivos>
  </soapenv:Body>
</soapenv:Envelope>
```

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

<SOAP-ENV:Envelope
xmlns:SOAP-ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:id="http://x-road.eu/xsd/identifiers" xmlns:xrd="http://x-road.eu/xsd/xroad.xsd">
<SOAP-ENV:Header>
[.....]
</SOAP-ENV:Header>
<SOAP-ENV:Body>
<getNacidosVivosResponse xmlns="http://api.minsal.gob.sv/producer">
<request>
<fecha_registro>2017-02-01</fecha_registro>
</request>
<response>
<array>
<fecha_nac>2017-01-31</fecha_nac>
<madre_dept>4</madre_dept> <establecimiento>163</establecimiento>
<madre_munic>0405</madre_munic> <sex_nac>M</sex_nac>
<madre_canton>634</madre_canton>
<madre_edad>29</madre_edad>
</array>
<array> <fecha_nac>2017-01-31</fecha_nac>
<madre_dept>2</madre_dept> <establecimiento>72</establecimiento>
<madre_munic>0202</madre_munic> <sex_nac>F</sex_nac>
<madre_canton>ND</madre_canton>
<madre_edad>16</madre_edad>
</array>

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

~# curl -v -H "Accept:text/xml" -X POST http://localhost:8080/adaptador-rest/Consumer/pruebas/getNacidosVivos/v1/?fecha_registro=2017-02-03

~# curl -v -H "Accept:application/json" -X POST http://localhost:8080/adaptador-rest/Consumer/pruebas/getNacidosVivos/v1/?fecha_registro=2017-02-03

< HTTP/1.1 200 OK
* Server Apache-Coyote/1.1 is not blacklisted
< Server: Apache-Coyote/1.1
< X-XRd-UserId: anonymous
< X-XRd-MessageId: 264e3f92-30e4-4c1e-84f7-b02323410717
< Content-Type: application/json;charset=utf-8
< Transfer-Encoding: chunked
< Date: Thu, 25 May 2017 16:06:06 GMT
<
[{"fecha_nac":"2017-02-02","madre_dept":1,"establecimiento":575,"madre_munic":"0107","sex_nac":"F","madre_canton":"ND","madre_edad":22},{"fecha_nac":"2017-02-02","madre_dept":1,"establecimiento":575,"madre_munic":"0107","sex_nac":"F","madre_canton":"ND","madre_edad":24}, ….

java -jar asicverifier-1.0.jar /var/verificationconf/ /var/lib/xroad/request-0rHDhoFviD.asice
ASiC container Verification successful.

Signer
Certificate:
Subject: SERIALNUMBER=SV/prueba/GOB, CN=1001, OU=stpp, O=Gobierno de El Salvador, C=SV
Issuer: CN=Certificadora de Entidades de Gobierno, OU=Gobierno Electronico, O=Gobierno de El Salvador, C=SV Serial number: 4173
Valid from: Thu Apr 06 19:46:38 CST 2017
Valid until: Wed Apr 01 19:46:38 CST 2019
ID: MEMBER:SV/GOB/1001
OCSP response
Signed by:
Subject: CN=OCSP, OU=Certificadora de Servicios, O=Gobierno de El Salvador, C=SV
Issuer: CN=Entidades de Gobierno, OU=Gobierno Electronico, O=Gobierno de El Salvador, C=SV
Serial number: 4096
Valid from: Sat Jan 28 15:23:29 CST 2017
Valid until: Fri Jan 23 15:23:29 CST 2027
Produced at: Sat Apr 08 15:18:09 CST 2017
Timestamp
Signed by:
Subject: CN=sellado.stpp.gob.sv, OU=Gobierno Electronico, O=Gobierno de El Salvador, C=SV
Issuer: CN=Certificadora de Sellado, OU=Gobierno Electronico, O=Gobierno de El Salvador, C=SV
Serial number: 4096
Valid from: Sat Jan 28 15:23:22 CST 2017
Valid until: Fri Jan 23 15:23:22 CST 2027
Date: Sat Apr 08 15:40:59 CST 2017
Would you like to extract the signed files? (y/n) y
Created file message.xml

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

tenoli
CONECTANDO DATOS

EL SALVADOR
UNÁMONOS PARA CRECER

INICIO | SERVICIOS | RECURSOS

- Instar Pasarela Tenoli
- Gestión de Servicios
- Servicios SOAP/XML
- Servicios REST/JSON
- Bitácora de Acceso

Qué es Teno
Es una plataf al seguro a institucione datos. Tenoli adem s registros y se rmiten auditar todos an y reciben. Este erno Electrónico in ción de Transformaci retaria Técnica y de Planificación de la Presidencia.

Cómo funciona Tenoli?
Tenoli es una red de túneles cifrados (VPN) que permite el intercambio seguro de datos usando Internet y firma electrónica simple según el artículo 33 de la Ley de Firma Electrónica. Para mayores detalles, revise la descripción de los componentes de la plataforma y el proceso de intercambio de mensajes de la red.

Mi institución ya usa túneles VPN, por que usar Tenoli?
Es posible que existan ya túneles VPN para dar acceso a sus clientes autorizados. Por otro lado, para consumir datos su institución necesita coordinarse con la institución dueña del servicio y crear canales seguros de mutuo acuerdo. Esta coordinación se complica a medida crece el número de instituciones y servicios involucrados. Tenoli centraliza esa coordinación y garantiza un mecanismo común de intercambio seguro.

Qué tan segura es la red Tenoli?
Los túneles cifrados que ofrece la red están creados usando llaves asimétricas (RSA) de 2048 bits, el algoritmo de cifrado SHA256 (hashing), bajo el protocolo TLS 1.2. Es decir, el nivel de seguridad que se obtiene al usar certificads de la red Tenoli es igual o más seguro que el cifrado que ofrecen otros productos VPN disponibles en el mercado.

SECRETARÍA Y DE PLANIFI DE LA PRESI
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

Lessons learned…

- Interoperability is not a technology issue, a data exchange solution alone is not going to solve our problems.

- Interoperability today, specially within government, demands the creation of ontologies, information domains and integration clusters.

- Technology must not get on the way, the simpler the solution the better (Do Less) [3]

3- Government Design Principles, https://www.gov.uk/design-principles

Final thoughts

- Digital transformation of government is not about tech, is about having an effective management strategy [6].

- We must learn and incorporate experiences into our own context, often best practices can not be replicated with the same level of success.

- There many new technologies that hopefully can be adapted to meet government needs in the near future e.g. Open ID Connect, Hyperledger ,etc. More Research is needed ..;)

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

6- Deloitte Digital,The Journey of Government Digital Transformation, 2015.

Useful Links

- http://tenoli.gobiernoelectronico.gob.sv/
- http://github.com/egobsv
- http://softwarepublicoregionalbeta.net/catalog/projects/Tenoli-LAT
- https://github.com/ria-ee/X-Road

Eric Ramirez, eramirez@presidencia.gob.sv

SECRETARÍA TÉCNICA Y DE PLANIFICACIÓN DE LA PRESIDENCIA
GOBIERNO DE EL SALVADOR
UNÁMONOS PARA CRECER

MUCHAS GRACIAS

EL SALVADOR
Grande como su gente

SECRETARÍA TÉCNICA
Y DE PLANIFICACIÓN
DE LA PRESIDENCIA
GOBIERNO DE
EL SALVADOR
UNÁMONOS PARA CRECER

/SETEPLANSV

@SETEPLAN_SV

Eric Ramirez, eramirez@presidencia.gob.sv