

E-governance e Cybersecurity

Workshop

Quadro Político e Regulamentar para a Cybersegurança e PICI

Eixos do e-gov em CV





Gov-Cidadão e Gov Empresas

- postura dos agentes públicos, focalizada nas necessidades dos cidadãos utentes.
- reformulação da maneira de lidar com o “cliente” e com os “negócios”



Governo - Governo

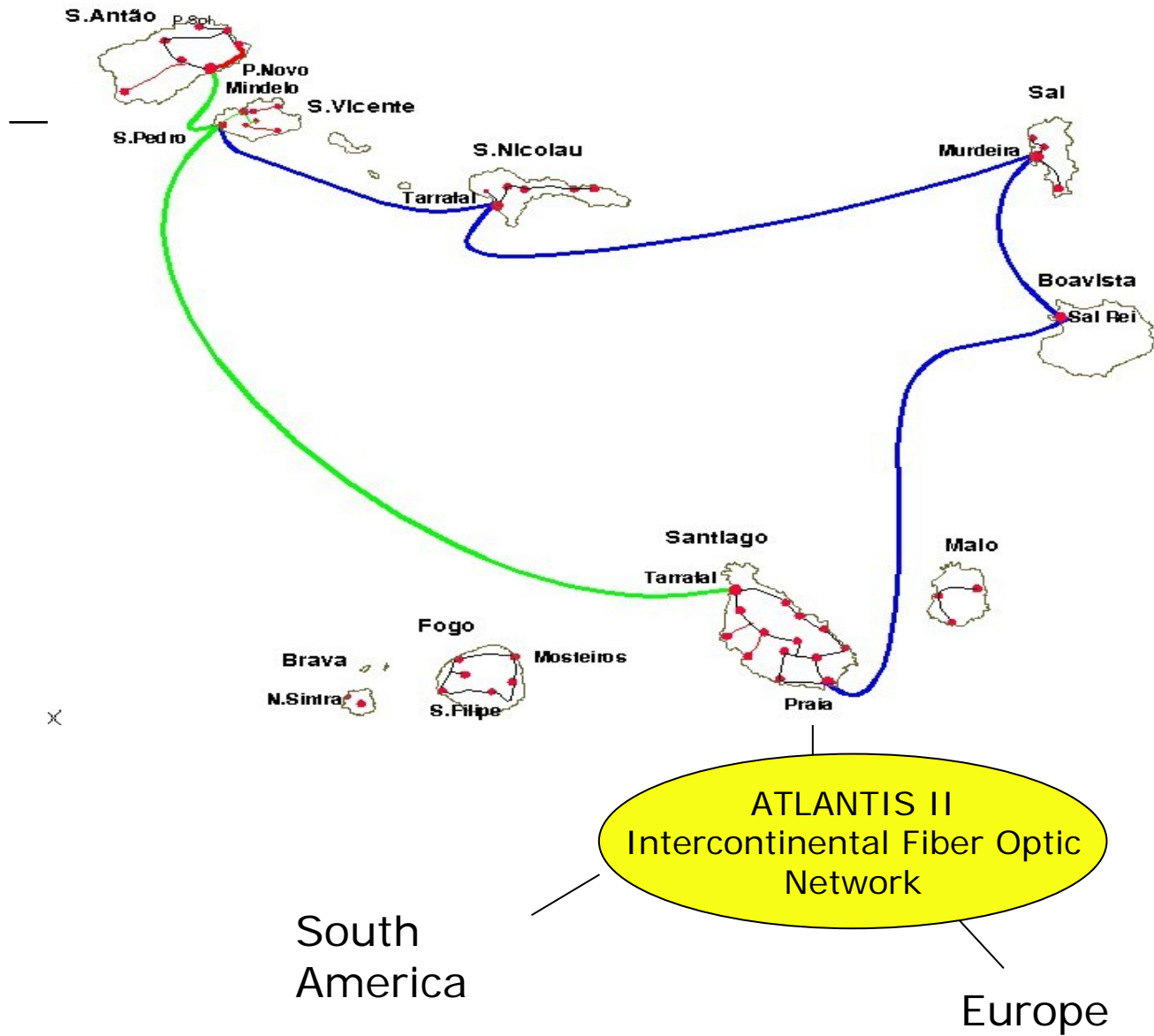
- Cria as condições organizacionais, humanas e tecnológicas para a qualificação da máquina pública
- Responder aos novos paradigmas da prestação pública, conferir eficiência e eficácia
- Criar uma cultura de efectiva colaboração horizontal entre os departamentos



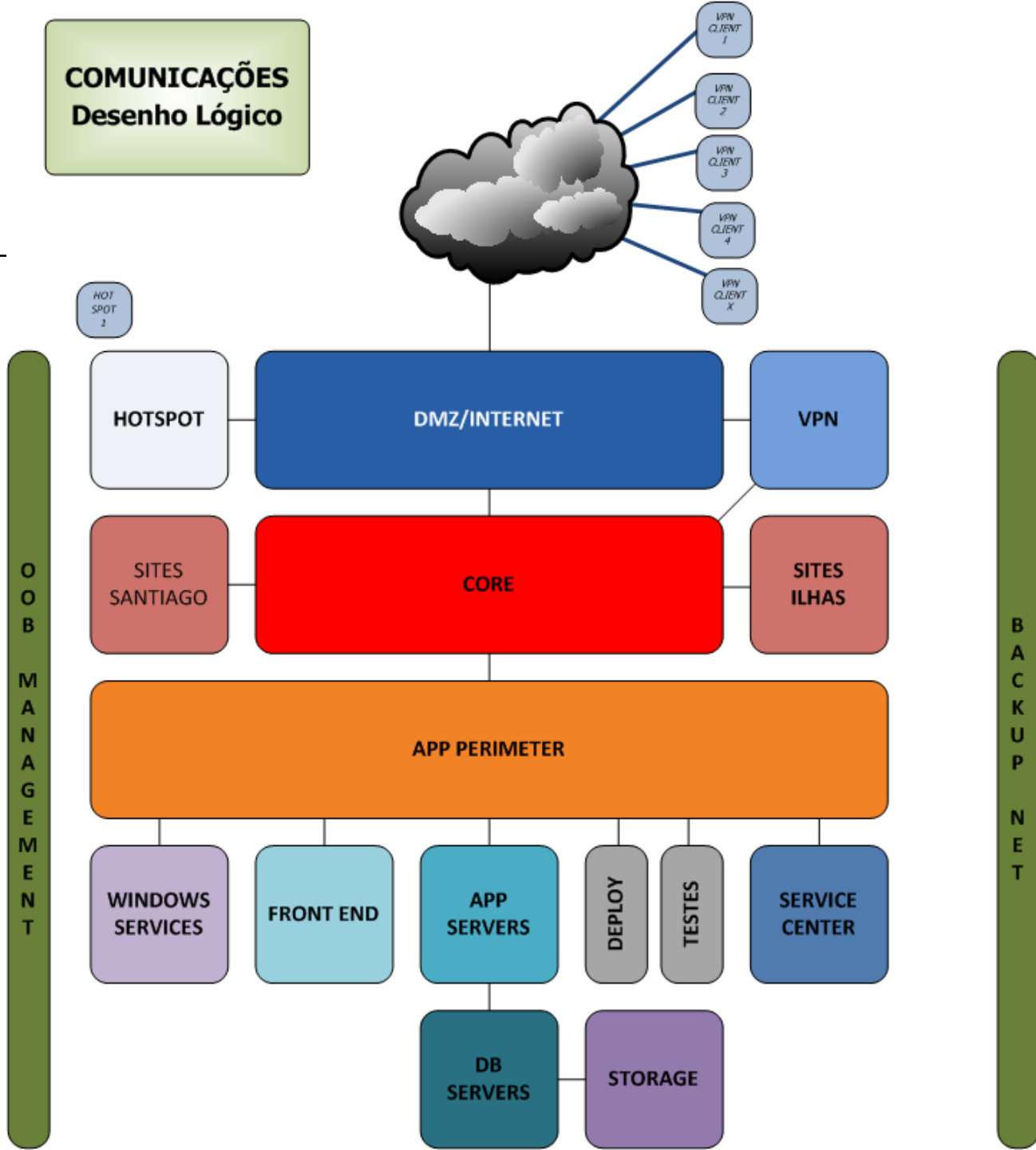
Governança electrónica

Componentes

Fiber Optic Infrastructure



COMUNICAÇÕES Desenho Lógico



Governança Electrónica-Serviços

- EMAIL – com certificados digitais
- Hosting e Housing – Páginas, serviços e servidores
- Hotspots
- INTERNET – Comunidades e Forums de discussão
- Serviços de Identificação – BI, Passaporte, Residência, Registos e Notariado
- Serviços Financeiros – Orçamento Geral do Estado, Orçamentos Municipais
- Serviços da Educação – Acesso ao Ensino Superior



Governança Electrónica-Serviços

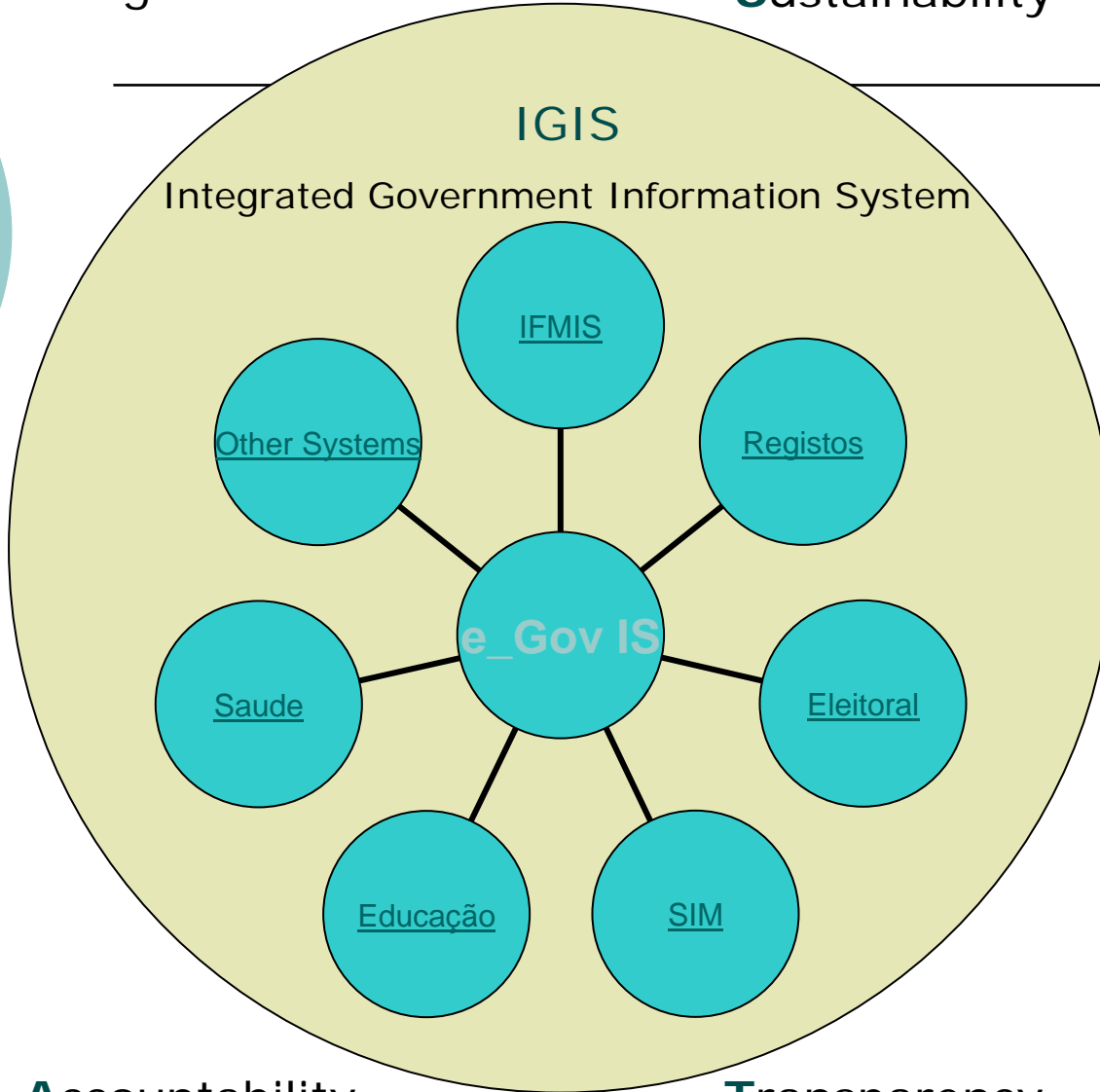
- Serviços Eleitorais – Recenseamento, Eleições
- Serviços da Saúde – Gestão de Stock, marcação de consultas
- Serviços do Poder Local – Gestão Municipal
- Serviços de Gestão de território - SIG
- Serviços Integrados – Projecto Casa do Cidadão



Security

Integration

Sustainability



Accountability

Transparency

IDENTIFICATION & AUTHENTICATION

ELECTRONIC PAYMENT SYSTEMS

CABO VERDE DIGITAL





República de Cabo Verde
Republic of Cape Verde

CABO VERDE

CARTÃO DO CIDADÃO | CITIZEN'S CARD

Apelido(s) | *Surname*

AZEVEDO

Nome(s) próprio(s) | *Given name(s)*

SOFIA

Sexo | *Sex*

F

Nacionalidade | *Nationality*

CV CABOVERDEANA

Data de nascimento | *Date of birth*

11.06.1980

Altura | *Height*

1,55 m

Número de Identificação Civil | *I.D. number*

012345678

Validade | *Date of expiry*

11.06.2010

Assinatura do titular | *Holder's signature*



WWW – The Highway



-
- Web Oriented Access (n tier Architecture)
 - PKI Infrastructure



Paper free Execution - Aposta na Desmaterialização

Physical Archive

Srv1

Srv1

Srv1

Srv1



República de Cabo Verde
Gabinete do Primeiro-Ministro
Comissão Interministerial para Inovação e Sociedade de Informação

Núcleo Operacional da Sociedade de Informação

CONTRATO Nº/2004

Entre o Núcleo Operacional da Sociedade de Informação – NOSI, representado pelo seu Gestor, nomeado pelo Despacho nº 07/2003 do Primeiro-Ministro, o Eng.º, adiante designado por primeiro outorgante e, de nacionalidade cabo-verdiana, residente na cidade da Praia, como segundo outorgante, é celebrado o presente Contrato nos termos seguintes:

Artigo 1
Objecto

Execução Financeira

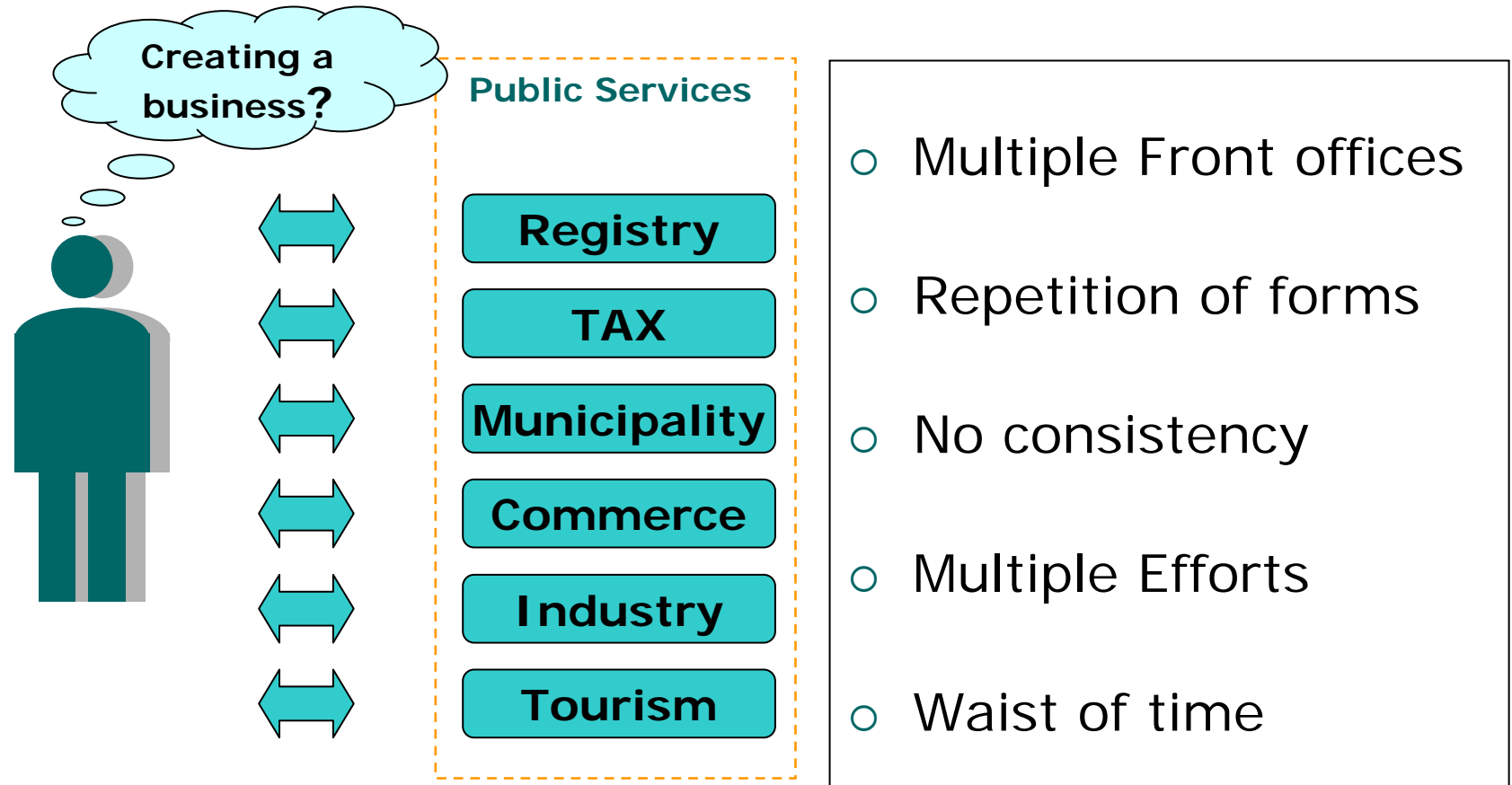
Certidões Online
Empresa no dia

Central Bank

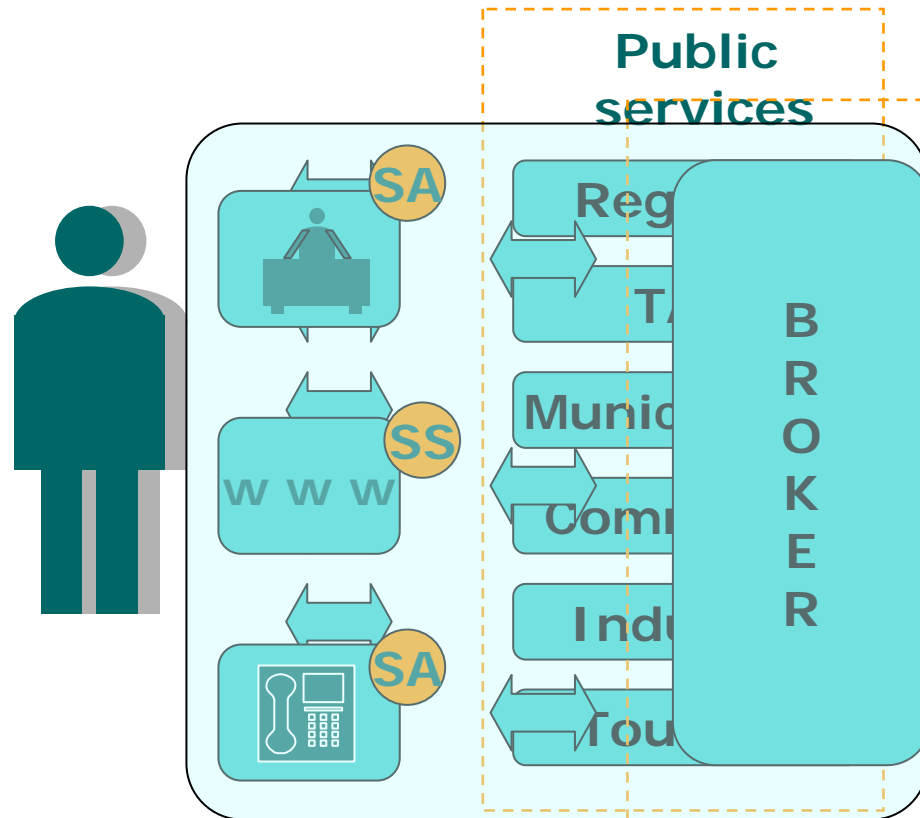
Electronic Relationship

E-Archive

Modelo Actual de Atendimento



Modelo Actual de Atendimento



- Multiple Front offices
- Repetition of forms
- No consistency
- Multiple Efforts
- Waist of time



Segurança na Internet

Visão internacional



Potencialidades e riscos

- Internet oferece aos utilizadores possibilidades e potencialidades de consulta e criação de grandes quantidades de informação gerando-lhes oportunidades
- Segurança na Internet - um elemento essencial para a segurança dos utilizadores das TIC
- O potencial da Internet nas relações económicas e comerciais requer um ambiente que garanta confiança e uma plataforma estável e segura

Medidas globais para a segurança

- Procura-se hoje reunir esforços para resolver o problema da segurança internacional da Internet, nomeadamente o cyber-terrorismo e o cyber-extremismo
- No IGF II o Conselho da Europa recomendou a aplicação de diversas Convenções internacionais respeitantes a:
 - Cybercriminalidade
 - Prevenção contra o terrorismo
 - Protecção de pessoas e o tratamento automatizado de dados pessoais
 - Tráfego de pessoas
 - Protecção de crianças contra exploração e abusos sexuais

Medidas globais para a segurança

- Atenção particular à “Convenção sobre a protecção das crianças contra a exploração e abusos sexuais” que devia estar aberto a assinatura de todos os Estados, europeus ou não, em Outubro de 2007
- A Convenção obriga os Estados a criminalizar condutas como o acesso deliberado à pedopornografia na Internet e a aproximação de crianças para fins sexuais
- Recomendação de banir a pornografia da porta normalmente utilizada para o tráfego Web e passá-la para uma porta reservada a tráfego para adultos

Cultura de segurança vs. cooperação na protecção

- Papel importante devem ter os poderes públicos na sensibilização e na promoção de uma cultura de segurança na Internet
- Os esforços nacionais e regionais não são suficientes para para uma luta eficaz contra problemas como a difusão de vírus por correio electrónico ou a cibercriminalidade
- Considerando a natureza transfronteiriça do fenómeno torna-se necessário mobilizar a cooperação internacional para mecanismos de intervenção internacionais



Cabo Verde

Governança electrónica e gestão do bem informação

O bem “informação”

- Mais do que um conjunto de dados que, em si, têm pouco significado
- Os dados só se tornam num recurso de valor para qualquer organização (Estado) quando transformados em informação
- Informação – bem com valor primordial e como tal deve ser protegida e cuidada através de políticas e regras da mesma forma e intensidade que os recursos financeiros, materiais e outros



Informação e suas propriedades

- Confidencialidade, integridade e disponibilidade – propriedades que orientam a análise, planeamento e implementação da informação
- Legitimidade e autenticidade – propriedades implicadas na realização de transações comerciais através de redes electrónicas privadas ou públicas

Acesso à informação

- O acesso à informação da RPE é individual e intransferível
- Só pode acontecer através de identificação e autenticação do utilizador
- Só pode acontecer mediante autorização prévia
- O acesso é exclusivo às informações necessárias para o desempenho profissional no âmbito das atribuições e responsabilidades do utilizador



Informação e segurança

- Como activo crítico que é, deve estar sujeita a regras e procedimentos e ter uma estrutura de protecção
- A sua protecção é da responsabilidade de cada um dos agentes independentemente do seu posicionamento hierárquico
- A segurança da informação não é um simples produto ou tecnologia que se pode adquirir e aplicar



Informação e segurança

- Deve ser encarada de forma integrada com o “negócio”, como um processo em permanente evolução com potencial para provocar e gerir mudanças nos hábitos, comportamentos, estruturas organizativas e infra-estruturas tecnológicas



Propriedade da Informação

- O Estado de Cabo Verde é o proprietário das informações armazenadas, processadas e transmitidas através da sua rede privada

Correio electrónico

- As mensagens de correio electrónico são instrumentos de comunicação interna e externa para a realização das actividades funcionais do Utilizador
- O uso do correio electrónico é pessoal, intransmissível, inerente a função e o utilizador é responsável por toda mensagem enviada a partir do seu endereço electrónico.
- O conteúdo do correio electrónico de cada utilizador somente pode ser acedido por terceiros mediante situação legal definida em legislação específica sobre este tema.

Ambiente da internet

- O ambiente de Internet deve ser usado para o desempenho das actividades profissionais do Utilizador
- Os sítios da Internet que não contenham informações que agreguem valor acrescentado ao exercício das actividades do Utilizador, conforme suas atribuições, não devem ser acedidos.
- Os acessos realizados nesse ambiente são registados e podem ser monitorizados com o objectivo de garantir a disponibilidade da Rede Privada do Estado, bem como devem estar de acordo com a legalidade e a ética.



Internet e rede do Estado

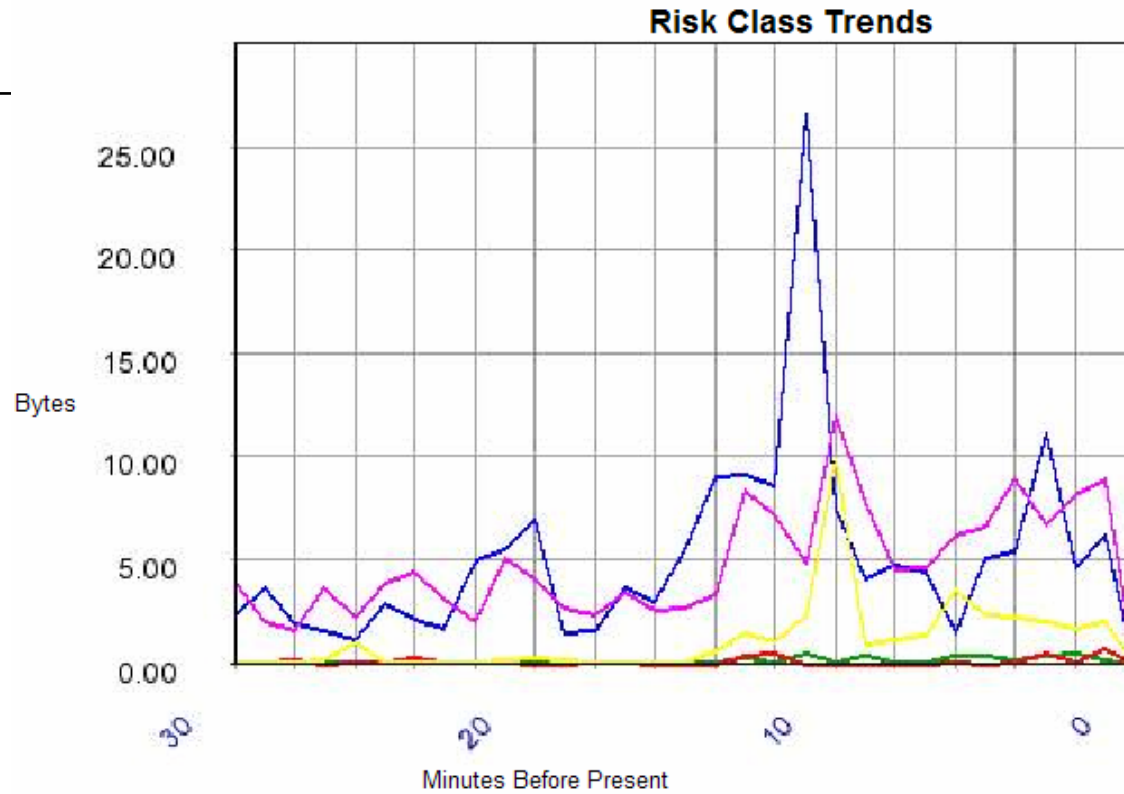
- É o ambiente virtual exterior à rede do Estado mas que se comunica com aquele por protocolos que permitem a troca de informações e a partilha de conhecimento
- xx/% de todo o tráfego do estado tem origem ou destina-se à internet








Medidas de Gestão e Segurança

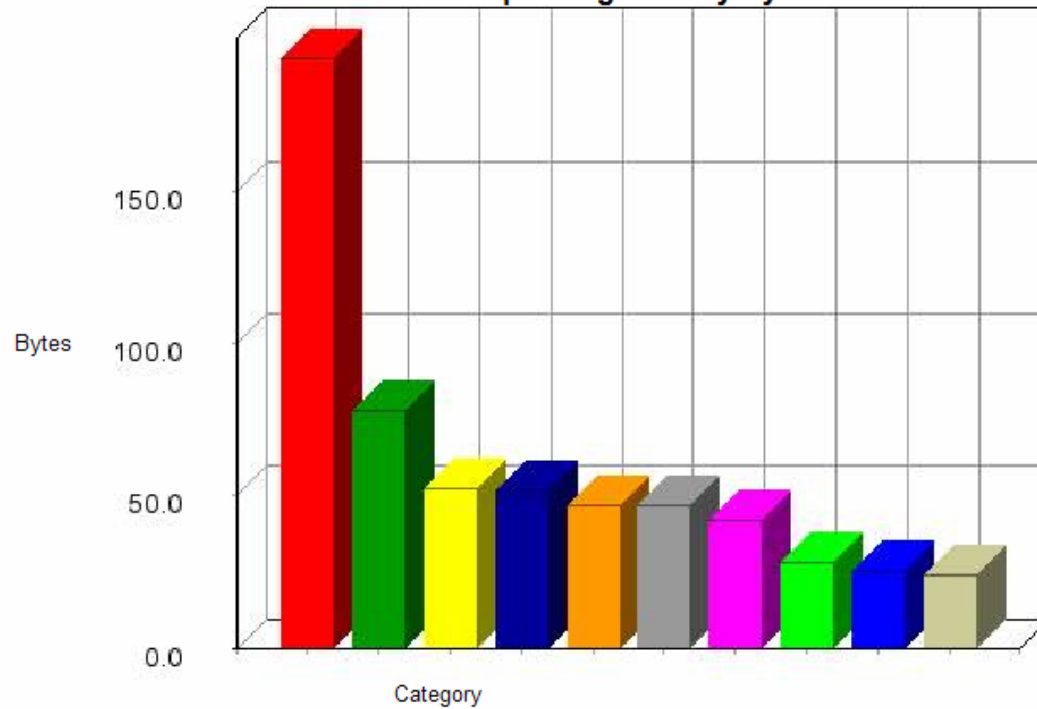
- Interactividade e transações seguras
- Sistemas de segurança física e lógica
- Infra-estruturas de chaves públicas





Risk Class	Bytes	Percent of Traffic
 Business Usage	166,339,949	33.8%
 Productivity Loss	156,100,365	31.8%
 Network Bandwidth Loss	37,187,239	7.6%
 Security Risk	3,687,208	0.8%
 Legal Liability	2,969,416	0.6%
Miscellaneous	125,273,583	25.5%

Top Categories by bytes



Category	Bytes (MB)
 Information Technology	193.4
 Miscellaneous	77.9
 Sports	52.2
 Information Technology: Search Engines and Portals	51.4
 News and Media	46.8
 Non-HTTP	46.6
 Miscellaneous: Private IP Addresses	41.9
 Society and Lifestyles: Social Networking and Personal Sites	27.8
 Productivity PG: Advertisements	25.2
 Bandwidth PG: Streaming Media	23.7

PKI – *Public Key Infrastructure*

Introdução

- PKI – Infra-estrutura de chaves públicas - é um processo que utiliza chaves públicas e privadas e certificados digitais para garantir a segurança do sistema e confirmar a identidade de seus utilizadores.
- Chave Pública – elemento de par de chaves assimétricas destinado a ser divulgado.
- Chave Privada – elemento de par de chaves assimétricas destinado a ser conhecido apenas pelo titular.
- Certificados digitais - são o elemento base de uma infra-estrutura de chaves públicas que se baseia na utilização de algoritmos de chaves assimétricas. Ou seja, um par de chaves, em que uma é denominada chave pública e a outra chave privada.

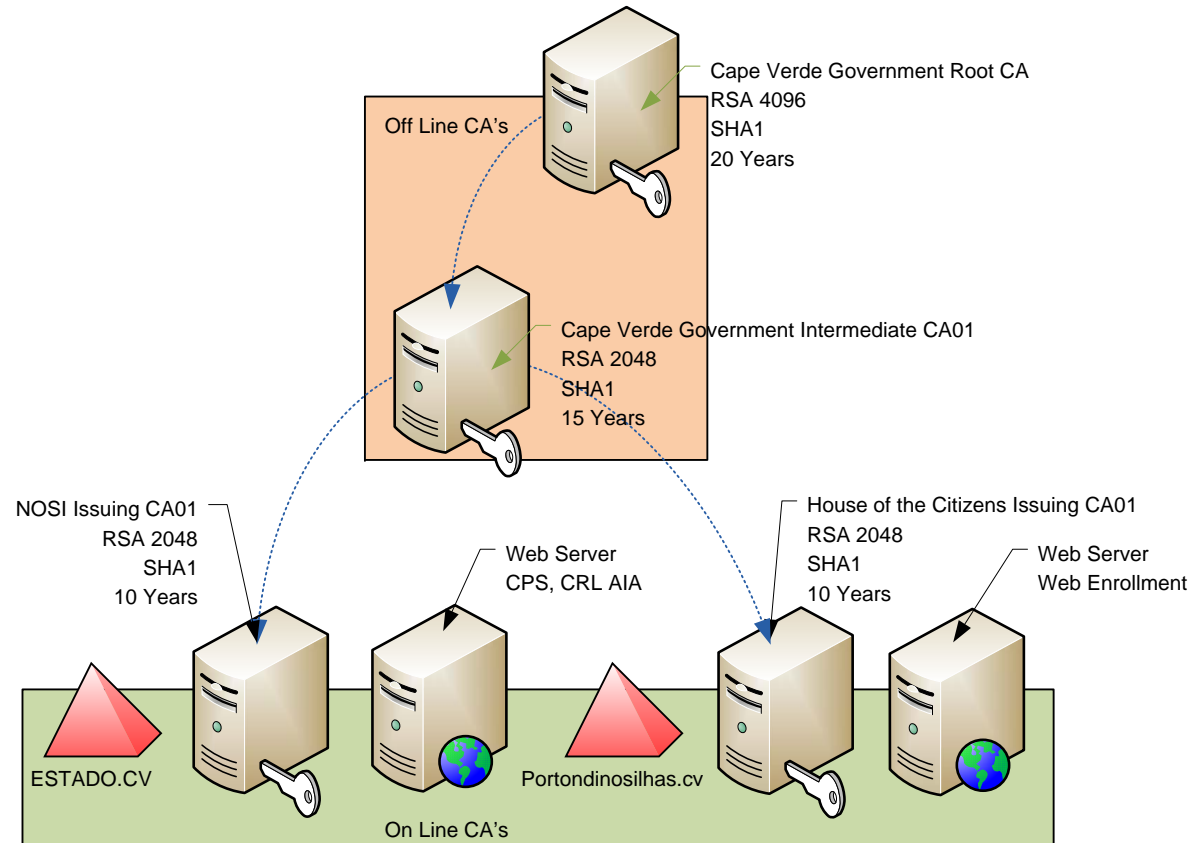
PKI – *Public Key Infrastructure*

Introdução

- Assinatura digital - baseado em sistema criptográfico assimétrico é composto por um algoritmo mediante o qual é gerado um par de chaves assimétricas exclusivas e interdependentes, uma das quais privada e outra pública.
- O titular usa a chave privada para declarar a autoria do documento electrónico.
- O declaratório usa a chave pública para verificar se a assinatura foi criada mediante o uso da correspondente chave privada e se o documento electrónico foi alterado depois de aposta a assinatura.

PKI – Public Key Infrastructure

Arquitectura PKI - NOSi





PKI – *Public Key Infrastructure*

Arquitetura PKI - NOSi

- *CA - Certification Authority* - entidade certificadora credenciada que cria ou fornece meios para a criação das chaves, emite certificados, assegura a respectiva publicidade e presta serviços relativos a assinaturas digitais.
- Uma CA é credenciada e fiscalizada por uma autoridade credenciadora. No caso NOSi, esta autoridade é a ANAC.



PKI – *Public Key Infrastructure* Implementação

- PKI nas máquinas
 - Certificados digitais nos Webserver (IIS e Apache) – maior segurança no acesso (https) no portal “Porton di nos ilhas”
 - Certificados no acesso a Outlook Web Access (email)
- PKI nos utilizadores
 - Certificados digitais no CNI



Improving Governance and Service Delivery through E-Government:

the Case of Cape Verde

Thank You