INTIC
Instituto Nacional de Tecnologias de Informação

UNIVERSIDADE FEDERAL
DE SANTA CATARINA

Identidade Electrónica e Certificação Digital

Estágio de Desenvolvimento, Desafios e Oportunidades

Prof. Ricardo Custódio, Dr., Março de 2023

INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação

Parcerias com INTIC e Moçambique

- Formação de Recursos Humanos
  - Graduação, Mestrado e Doutorado
- Infraestrutura de Chaves Públicas
- Empreendedorismo
  - Desenvolvimento de Aplicações
- Desafios da Identidade Eletrônica
- Assinador e Verificador de Assinatura

INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação

Experiências de ICP no mundo

- Acertos, erros, tecnologias
- Complexidade e Custos
  - Recursos Humanos Especializados
- Interoperabilidade
- Ameaças / Ataques
- Custo para os Usuários
- (In)Dependência Tecnológica
  - Longevidade
- **ICP como Infraestrutura**
  - **Simplificar - Simplicidade**
- **Inclusão - para TODOS**

Foco nas Aplicações

Identidade Eletrônica

Modelo de Dados no Sistema de Gestão de Identidades da Central

Com ela o cidadão pode se autenticar em serviços eletrônicos

Identificadores

Nome Completo
NUIT, no. RC, BI, etc …

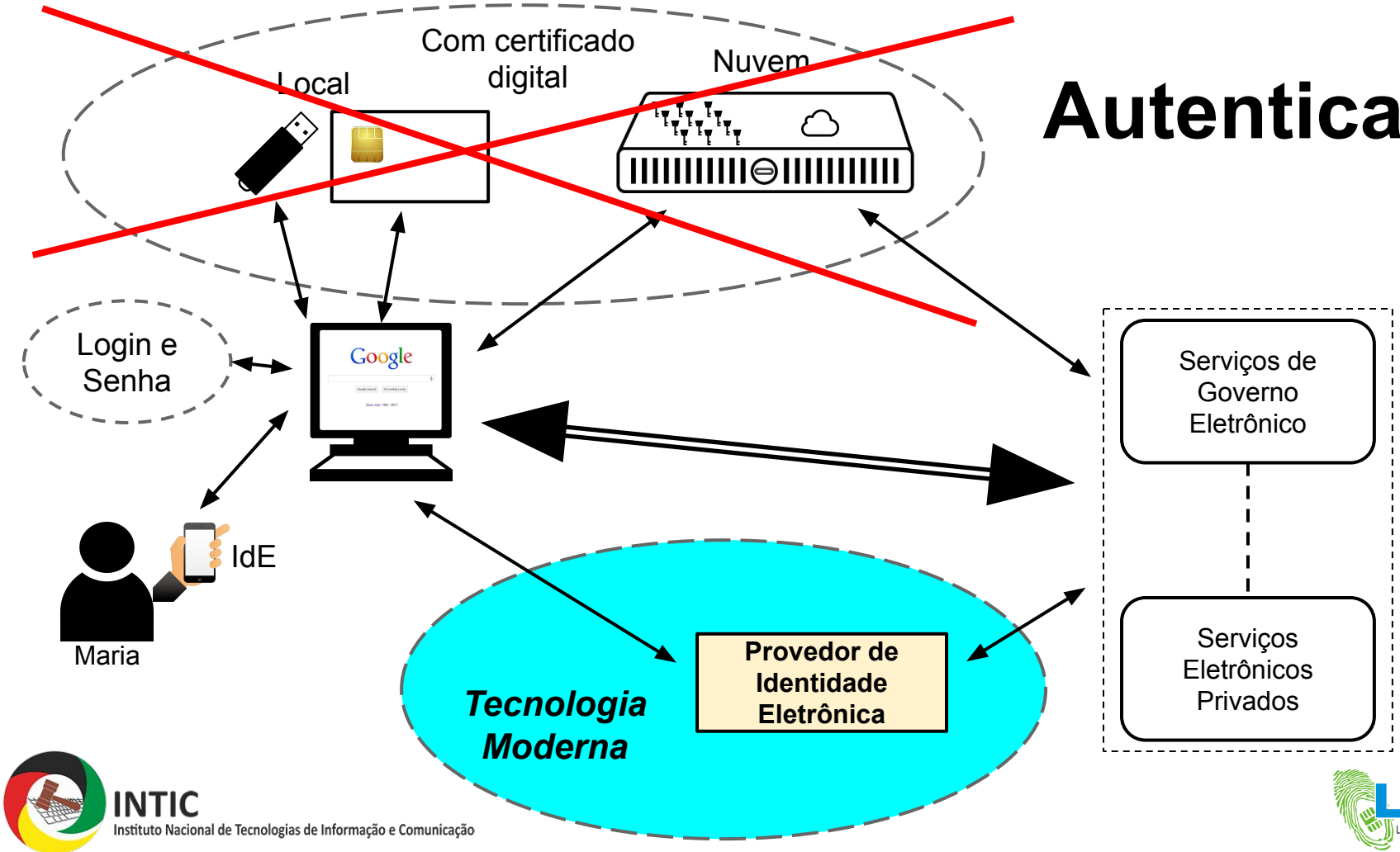
Credenciais

Senha
Outros Fatores de Autenticação

Atributos

Foto da Face
E-mail
Número do Celular
Endereço Residencial
Estado Civil
Nome da Mãe
Nome do Pai
Local de Nascimento
. . . . . .

Autenticação



Tipos de Assinaturas Eletrônicas

Tipo	Identificação do Signatário	Equivalência Automática à assinatura com reconhecimento de firma	Indicado para aplicações de
Simples	Sim, através de metadados	Não	Baixo risco
Avançada	Sim	Não	Alto risco
Qualificada	Sim	Sim	Alto risco e administração pública

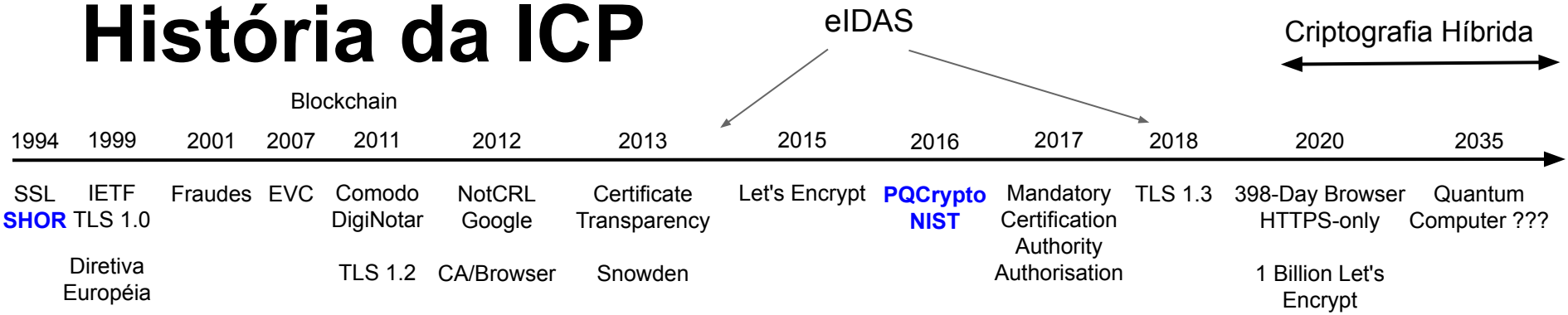
Certificação Digital

Segurança da Assinatura Eletrônica

*A assinatura eletrônica é **boa / útil** se for muito baixa a probabilidade do alegado signatário **negar** que assinou um dado documento eletrônico.*

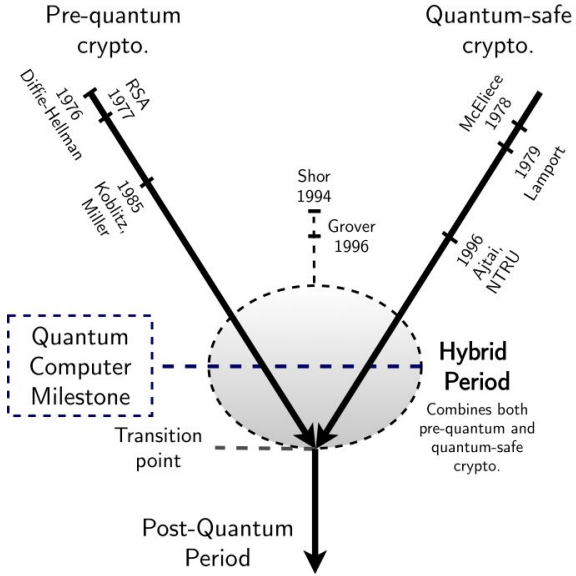
- Todos têm direito de negar uma assinatura
- Não há inversão do ônus da prova

História da ICP



Modelos de ICP

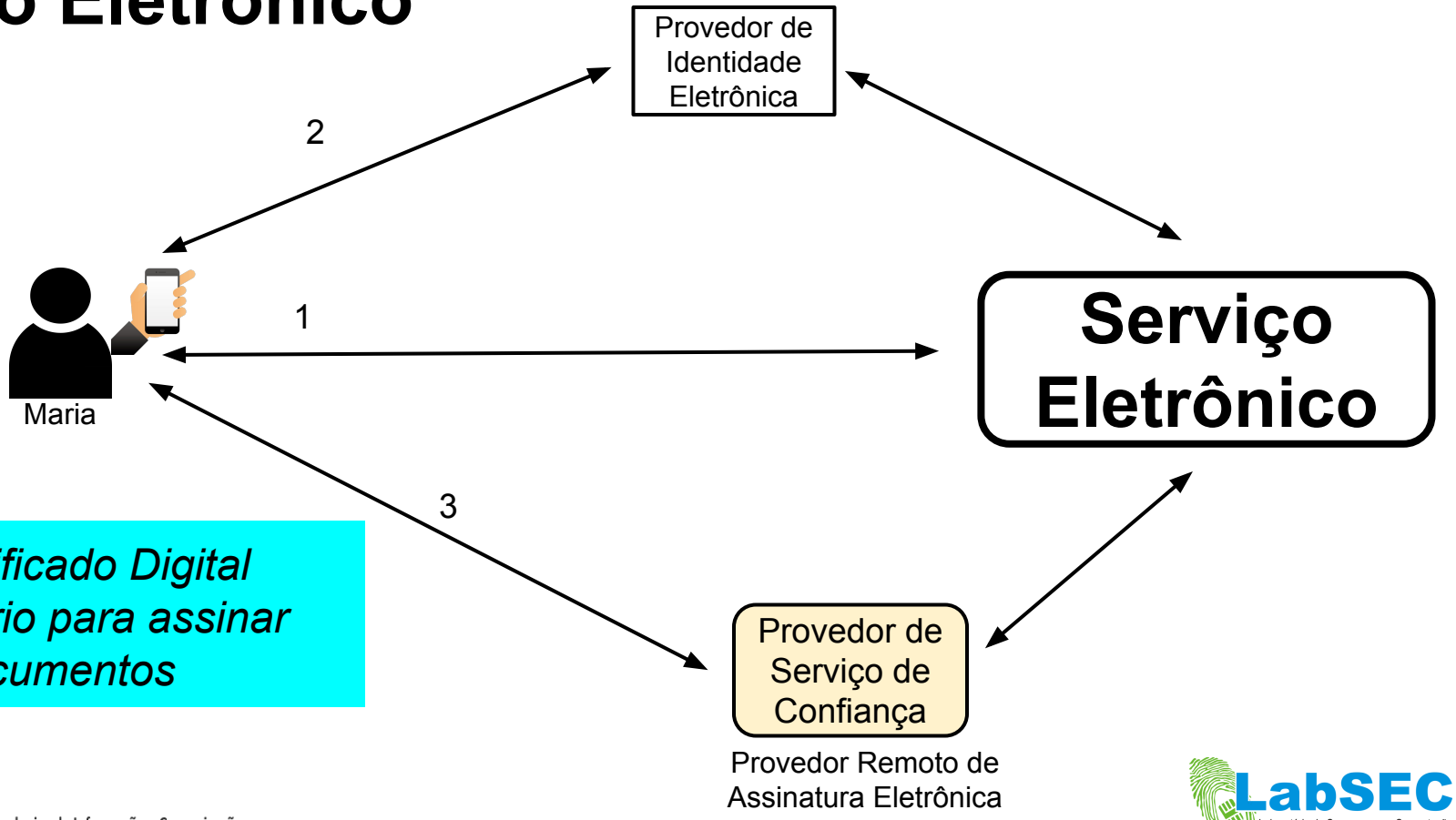
- PGP
- **X.509**
- Account Authority Digital Signature (AADS)
- Identity Based Encryption (IBE)
- SDSI
- SPKI
- Certificateless
- Blockchain based



INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação

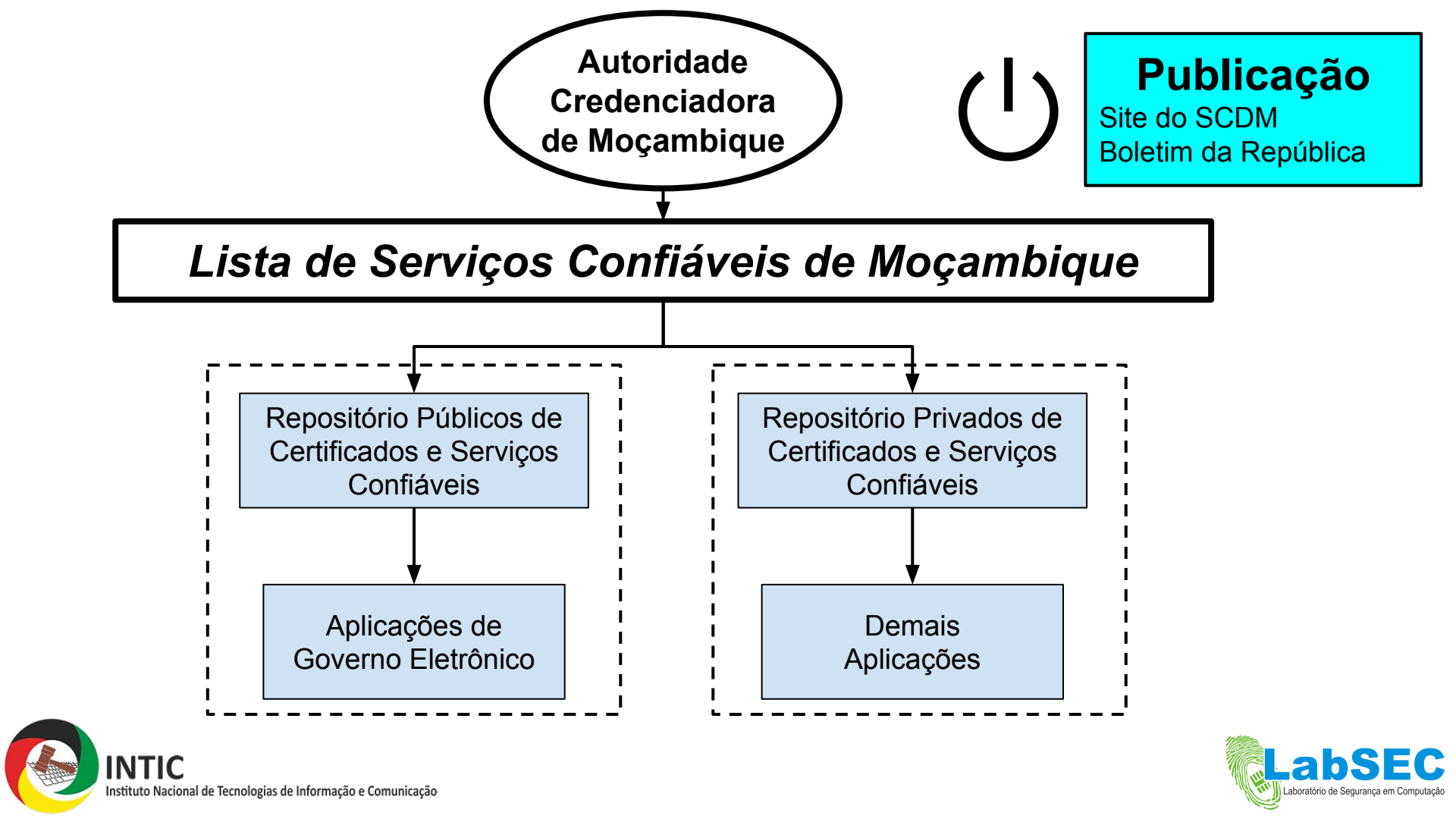
Serviço Eletrônico



O Certificado Digital necessário para assinar documentos

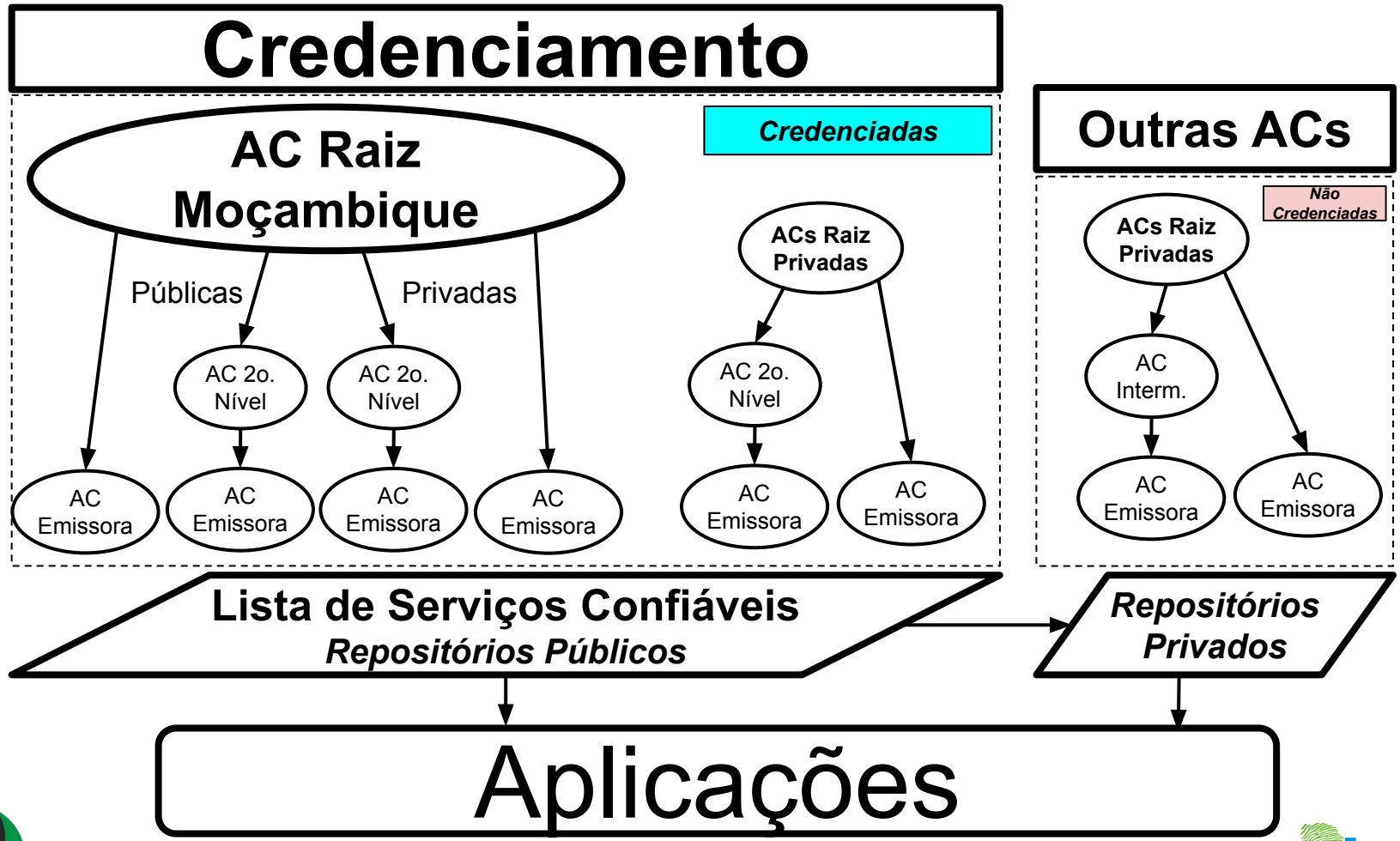
INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação



INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação



INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação

Assinador e Verificador de Assinatura de Moçambique

- **Válida** por, pelo menos, **100 anos**
- **Assinatura digital avançada** quanto como **assinatura digital qualificada**
- **Compatível** com os **sistemas legados**
- **Segura - chave privada exclusiva**
- **Não precisa**
  - **smartcards**
  - **tokens**
  - **certificado em nuvem**

Assinador e Verificador de Assinatura de Moçambique

- **Custo menor**
  - que os sistemas de assinatura tradicionais
- **Assinar e verificar assinaturas**
  - muito fácil, rápido e seguro
- **AR na forma de um**
  - Provedor de Identidades credenciado
- **Não precisa**
  - **software**
  - **extensões**
  - **plugins**

Assinador e Verificador de Assinatura de Moçambique

- **Acesso**
  - celular, notebook ou computador
- **Conhecimento / Consentimento / Comprometimento**
  - forma clara
  - simples
- **Artefato comprovante de verificação**
- **Somente os assinantes requeridos**
  - Privacidade

Assinador e Verificador de Assinatura de Moçambique

- **Confidencialidade / Sigilo**
  - Criptografia
  - Grupo de pessoas para a recuperação de documentos que foram cifrados
- **Não precisa de carimbo do tempo**
  - Certificado não precisa ser revogado

Assinador e Verificador de Assinatura de Moçambique

- **Fluxo da assinatura**
- **Voucher para assinantes não previamente registrados**
- **Os serviços de assinatura**
  - Programação de Aplicações (API)
- **À prova de todos os tipos de ataques conhecidos**
  - incluindo ataques quânticos
- **Preservação em longo prazo**

"A Simplicidade é o Ultimato da Sofisticação"
Autor desconhecido

Obrigado

Prof. Ricardo Custódio, Dr.
ricardo.custodio@ufsc.br

Brasileiro e
Moçambicano de Coração

INTIC
Instituto Nacional de Tecnologias de Informação e Comunicação

LabSEC
Laboratório de Segurança em Computação