ABIN

Presidência da República
Gabinete de Segurança Institucional
Agência Brasileira de Inteligência

Centro de Pesquisa e Desenvolvimento para a Segurança das Comunicações

CEPESC

ABIN

Agenda – Parte I

- A criptografia e uma breve história
- O CEPESC

Agenda – Parte I

- A criptografia e uma breve história
- O CEPESC

A criptografia

- A criptografia é uma arte milenar.
- O vestígio mais antigo de uma certa forma de criptografia foi descoberto escrito em uma tumba do grande chefe egípcio Khnumhotep II, por volta de 1900 a.C.

Motivação

Cifra de César:

A	B	C	D	E	F	G	H	...
D	E	F	G	H	I	J	K	...

ABIN ⟶ **DELQ**

Evolução tecnológica

- O computador revolucionou a criptografia

Agenda – Parte I

- A criptografia e uma breve história
- O CEPESC

O CEPESC

- Na década de 70 o Brasil sofria com a espionagem estrangeira.
- MRE + SNI + Academia (IME e UnB), criaram o projeto Prólogo em 1975.
- A criptografia do Brasil começou em uma sala cofre do Itamaraty.

O CEPESC

- Esse grupo cresceu em tamanho e relevância, culminando na criação do CEPESC em 1982.
- Pesquisa e desenvolvimento na área de criptografia e segurança cibernética.
- Desenvolvimento de diversas soluções de segurança da informação.

Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

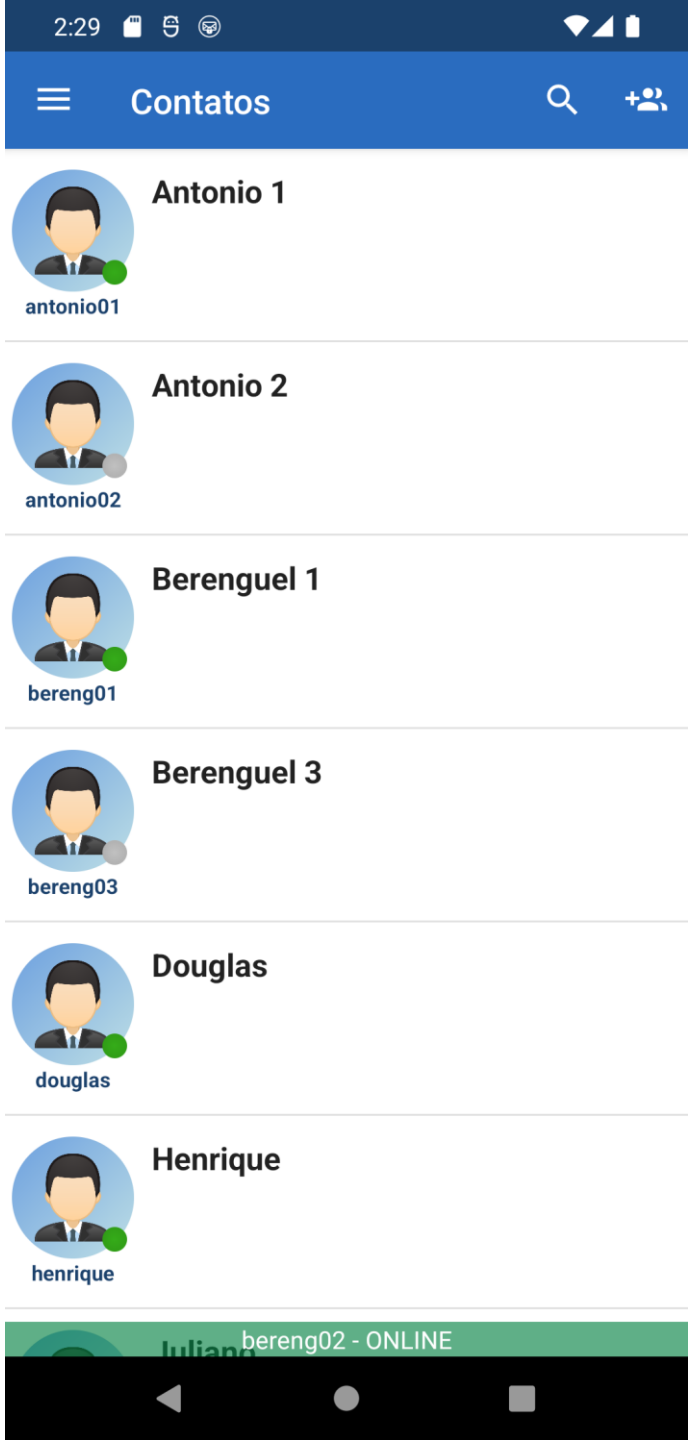
Sistemas de mensageria

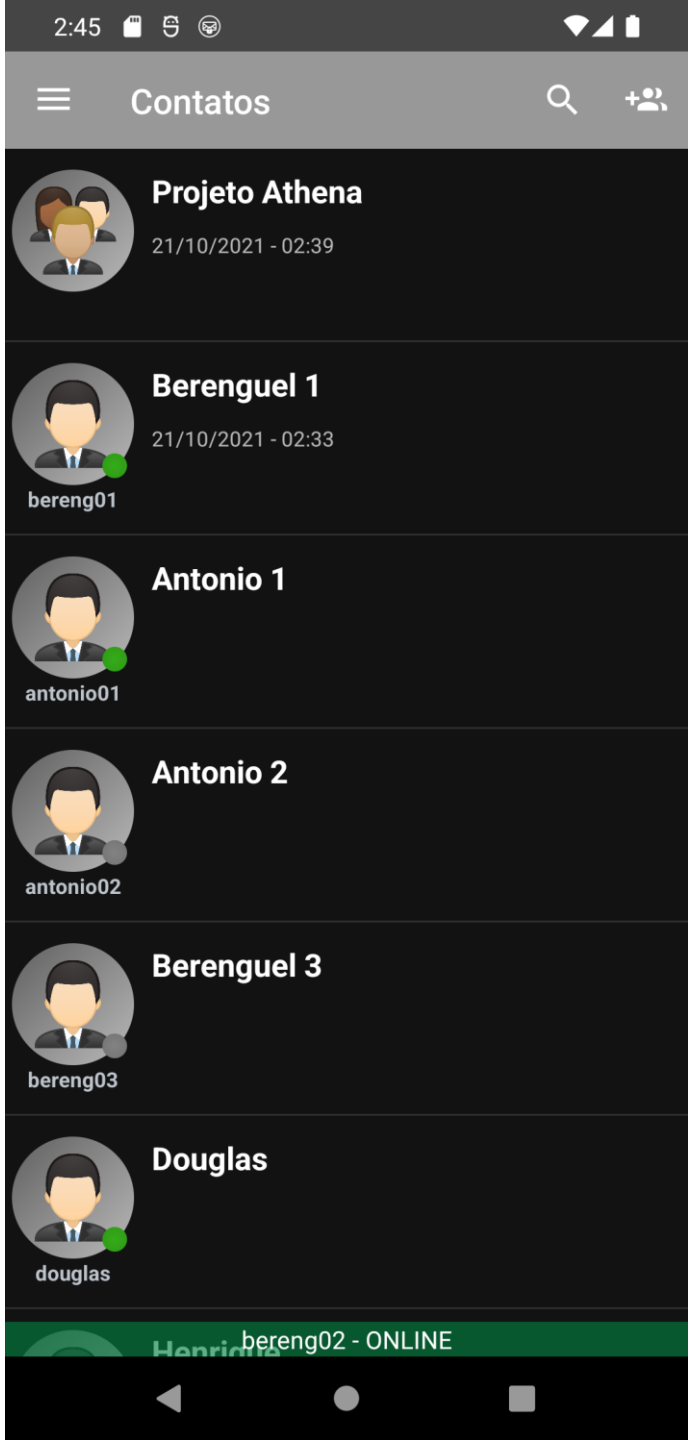
- Hoje, é muito comum utilizar serviços de mensageria como o Whatapp para tramitar informações de governo.
- Essa realidade implica em um problema grave de segurança e contrainteligência.

Aplicativo Athena

- Aplicativo de celular desenvolvido pela ABIN, que permite a troca segura de mensagens, áudios, vídeos, arquivos e fotos, Comunicação entre pares ou em grupo, chamada de voz.

Apresentação dos contatos

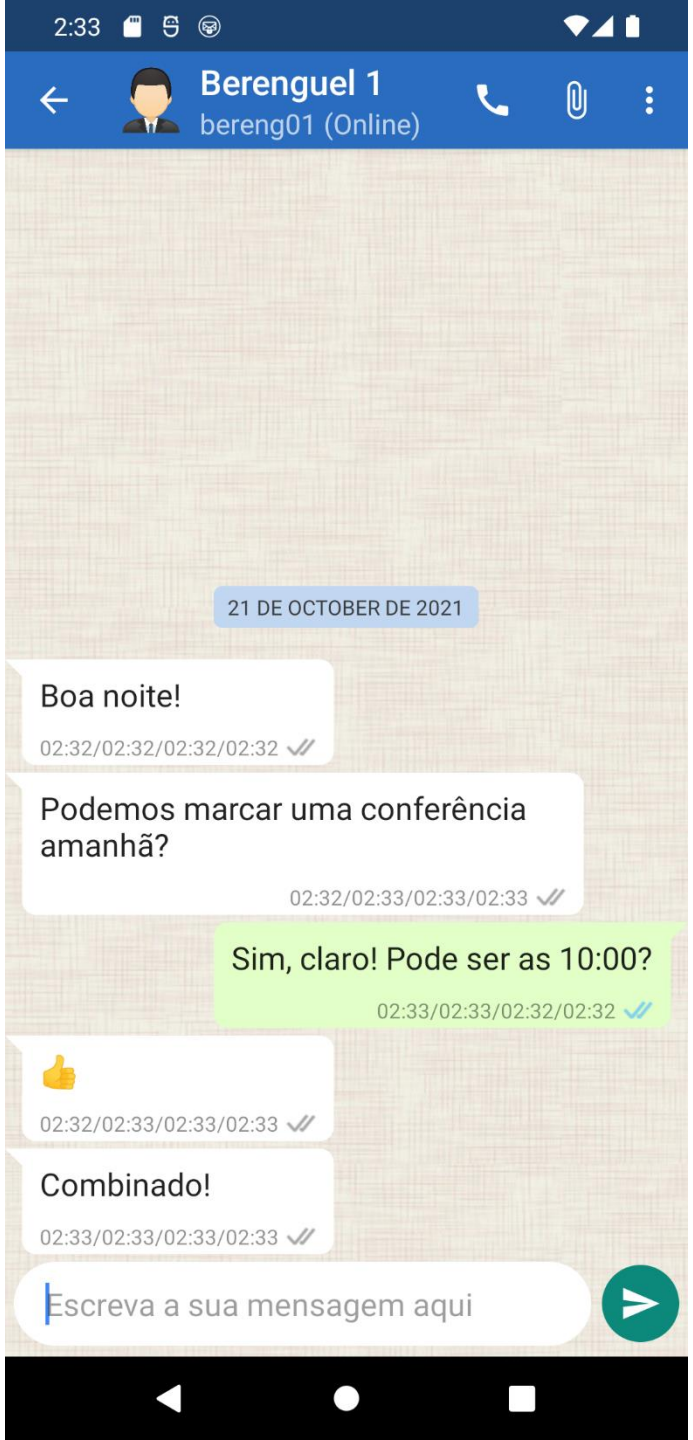


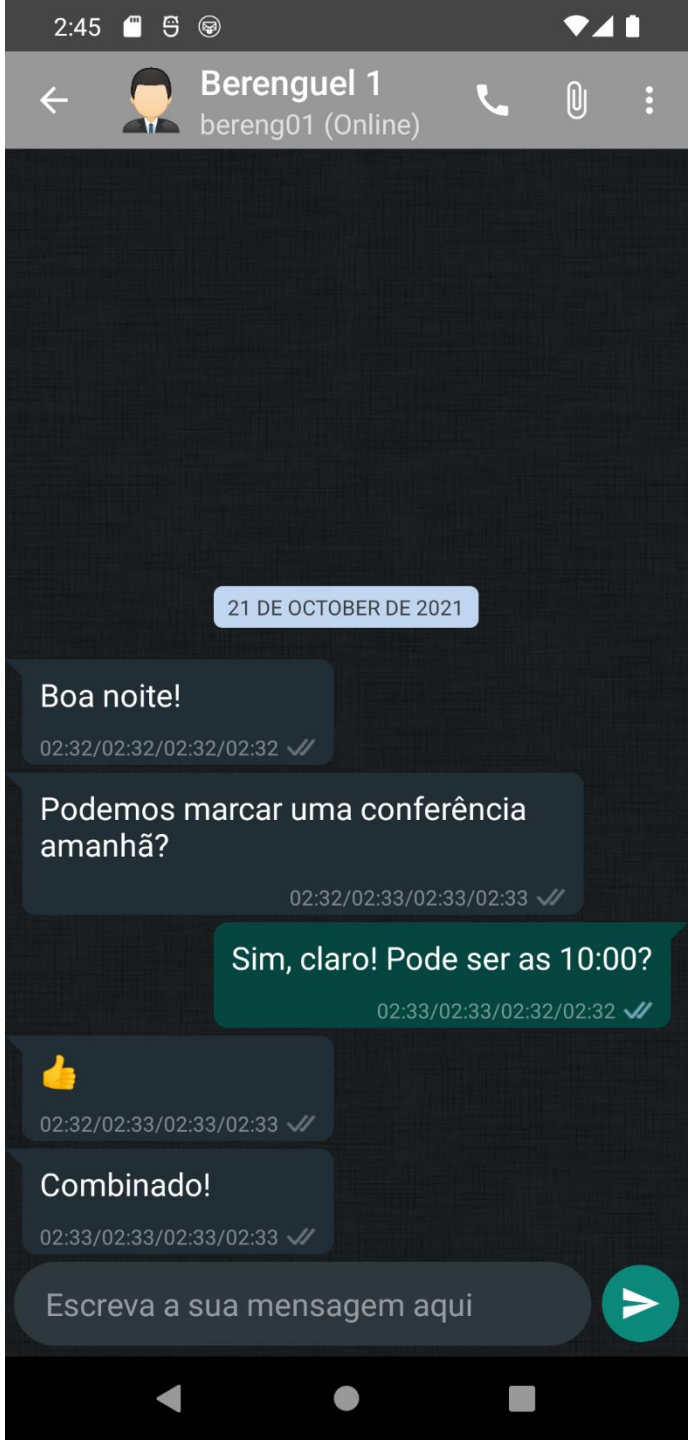


ABIN

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Conversas individuais



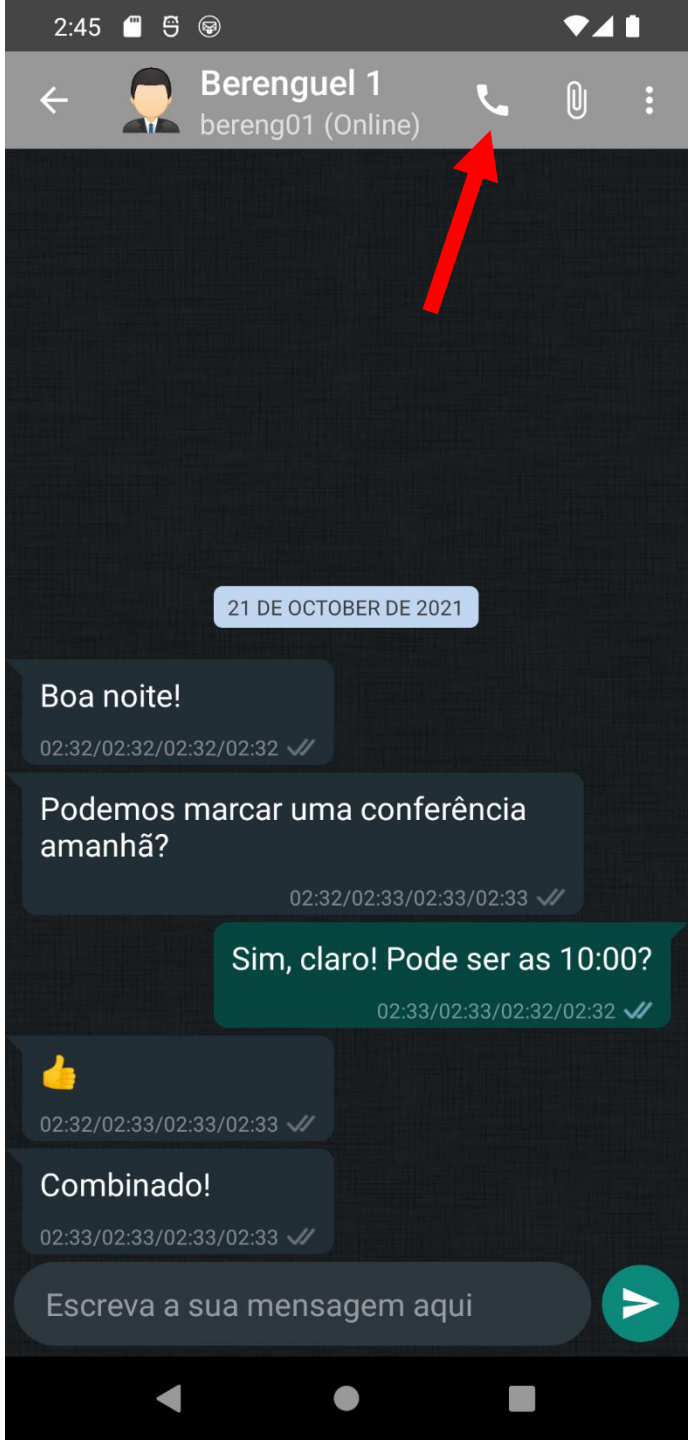


ABIN
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Conversas em grupos

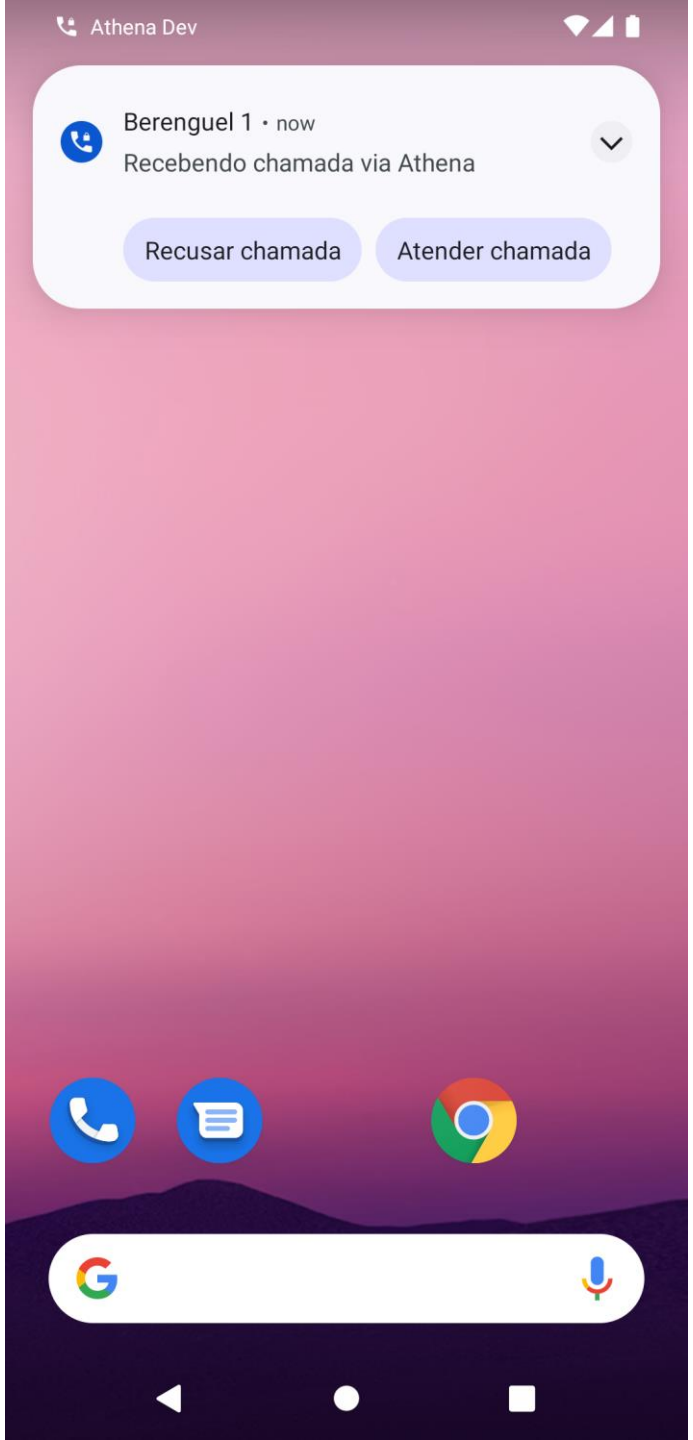
ABIN
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Chamada de voz



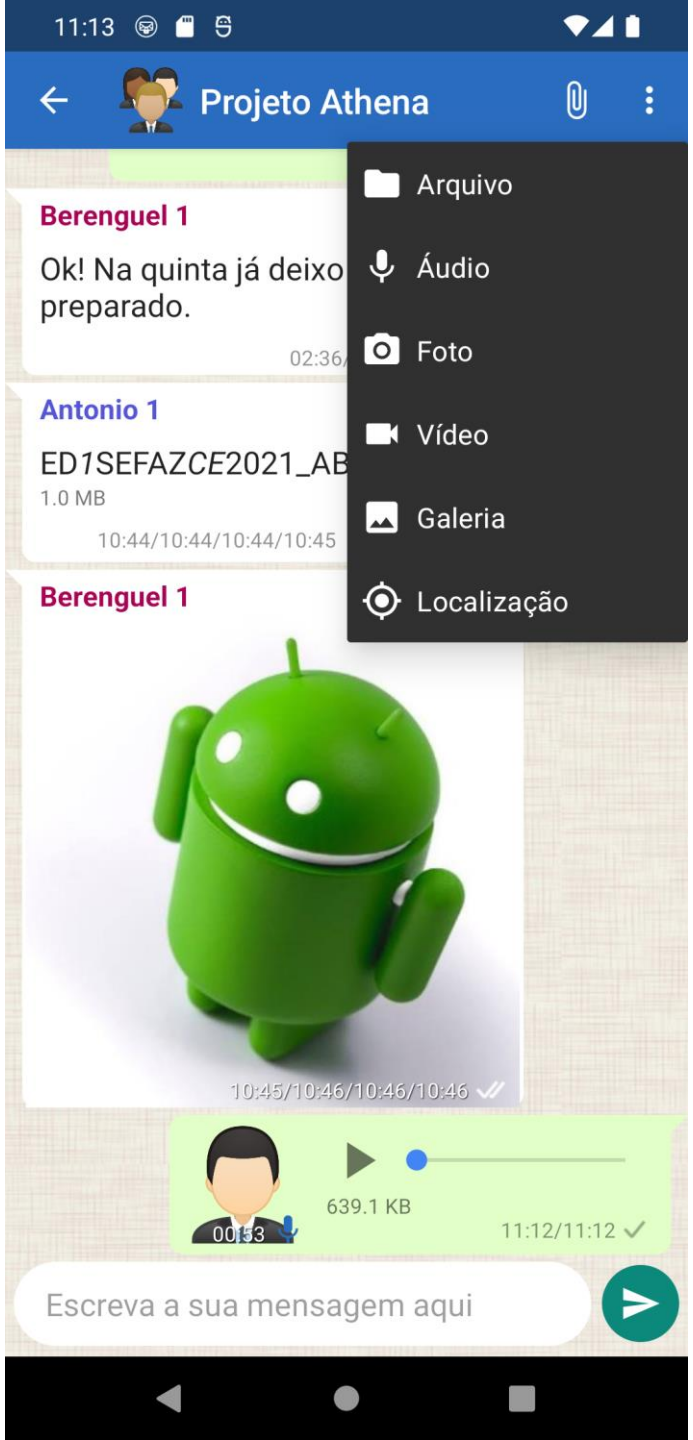
ABIN
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Chamada de voz



ABIN
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Tipos de dados para envio



ABIN
AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Athena - diferenciais

- Servidor próprio para a aplicação – não utiliza nuvem ou serviços de terceiros;
- Criptografia de Estado, desenvolvida pela ABIN para essa finalidade;
- Banco de dados criptografado no aparelho celular;
- Destruição do banco de dados de forma remota em caso de perda ou furto do celular;

ABIN

Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

Plataforma Criptográfica Portátil - PCP

- Túnel criptografado
- Algoritmo de Estado
- Criptografia em hardware
- Proteção contra tentativa de acesso
- Cifração de arquivos e assinatura digital
- Autenticação em sistemas
- Proteção contra infecção por vírus
- Volume criptografado
- Criptografia Pós-quântica

Plataforma Criptográfica de Alto Desempenho PCAD

- Túnel criptografado
- Algoritmo de Estado
- Criptografia em hardware
- Proteção contra tentativa de acesso

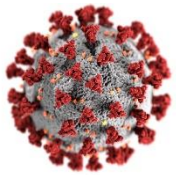
ABIN

Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

Efeito COVID-19



STJ teria sido vítima de ransomware; Ministério da Saúde sofre ataque

Ransomware pode ter criptografado todos os dados do STJ; vários sistemas do Ministério da Saúde estão fora do ar

Sistema do Tesouro Nacional sofre ataque hacker

Segundo o Ministério da Economia, a rede interna da secretaria do órgão foi alvo de um ataque de ransomware; a Polícia Federal foi acionada

Ransomware foi o ataque mais comum entre empresas brasileiras em 2021

16/08/2021 às 20:00 • 1 min de leitura

ABIN

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

Efeito COVID-19

- Os ataques cibernéticos aumentaram vertiginosamente desde o início da pandemia da COVID-19.
- A principal razão para isso é o uso indiscriminado de conexões de acesso remoto em sistemas críticos.
- Apesar da teórica segurança fornecida por uma VPN, na maior parte dos casos o atacante está a uma única senha fraca de conseguir acesso. Em outros, a própria VPN utilizada possui vulnerabilidades.

URUTAU

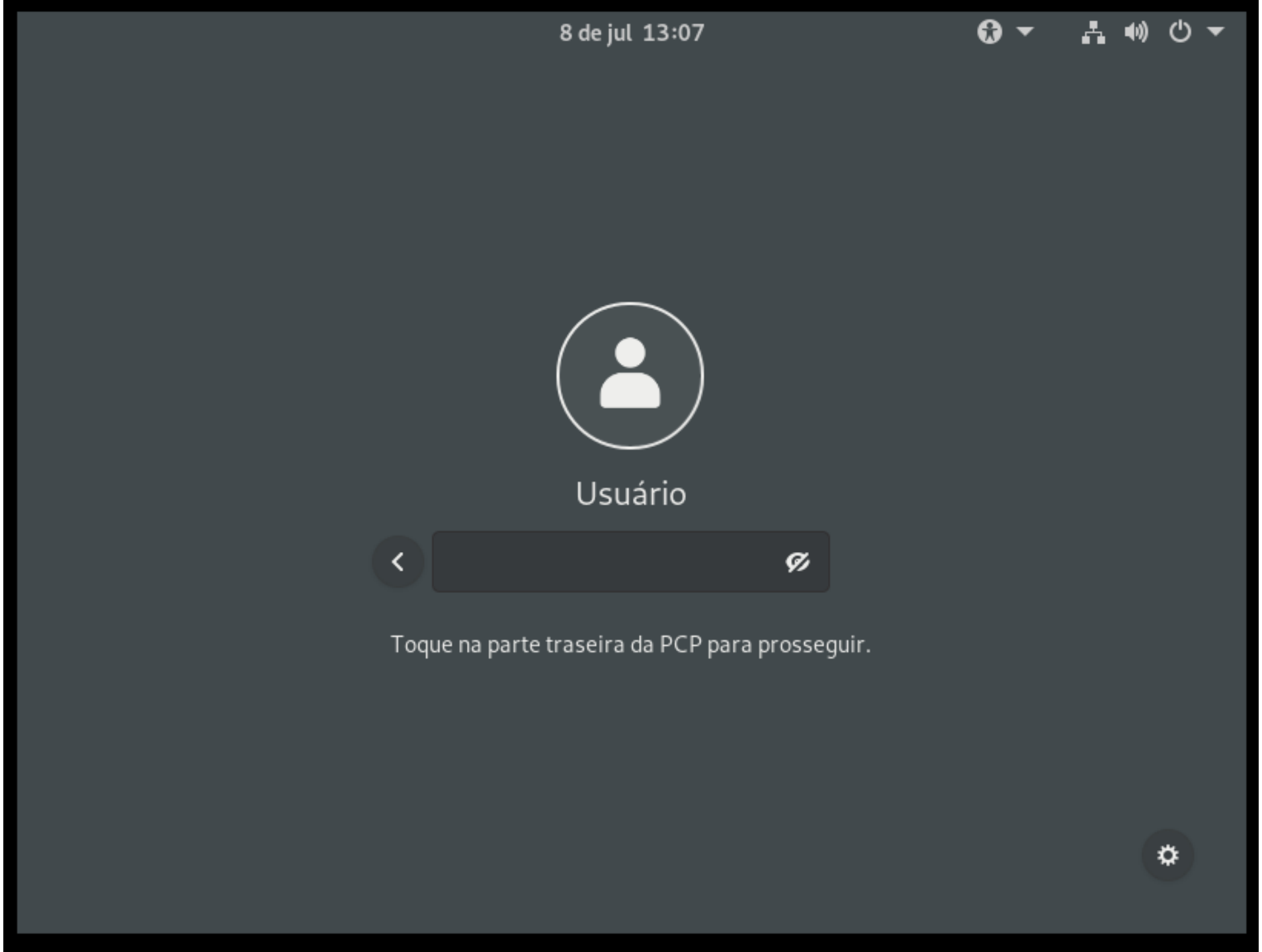
ABIN

AGÊNCIA BRASILEIRA DE INTELIGÊNCIA

URUTAU – Funcionamento da VPN

Processando, aguarde...

Senha p/ decifrar disco de dados:


8 de jul 13:07
Usuário
Toque na parte traseira da PCP para prosseguir.


29 de jun 11:09
VPN (Desconectada)
ÚLTIMO ACESSO:
Iniciou em 29/06/2021 às 10:45
Terminou em 29/06/2021 às 10:49
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


29 de jun 11:09
VPN (Desconectada)
ÚLTIMO ACESSO:
Iniciou em 29/06/2021 às 10:45
Terminou em 29/06/2021 às 10:49
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


29 de jun 11:20
VPN (Desconectada)
** PCP v3 foi INSERIDA **
ÚLTIMO ACESSO:
Iniciou em 29/06/2021 às 10:45
Terminou em 29/06/2021 às 10:49
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


8 de jul 12:53
VPN (Desconectada)
Conectar à VPN
ÚLTIMO ACESSO:
Iniciou em 07/07/2021 às 15:46
Terminou em 07/07/2021 às 16:00
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Windows + L = Bloquear a tela
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


29 de jun 14:35
VPN (Conectando 117...)
ÚLTIMO ACESSO:
Iniciou em 29/06/2021 às 14:24
Terminou em 29/06/2021 às 14:27
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


29 de jun 14:34
VPN (Conectada)
ÚLTIMO ACESSO:
Iniciou em 29/06/2021 às 14:24
Terminou em 29/06/2021 às 14:27
ATALHOS:
Windows + N = Acesso à Internet
Windows + C = Acesso à Intranet
Ctrl + Shift + Alt + Del = Formatar o disco
INTRA


Insira as credenciais de autenticação RDP
Nome de usuário
12069
Senha
Domínio
abinnet
Salvar senha
OK
Cancelar

URUTAU – Vantagens

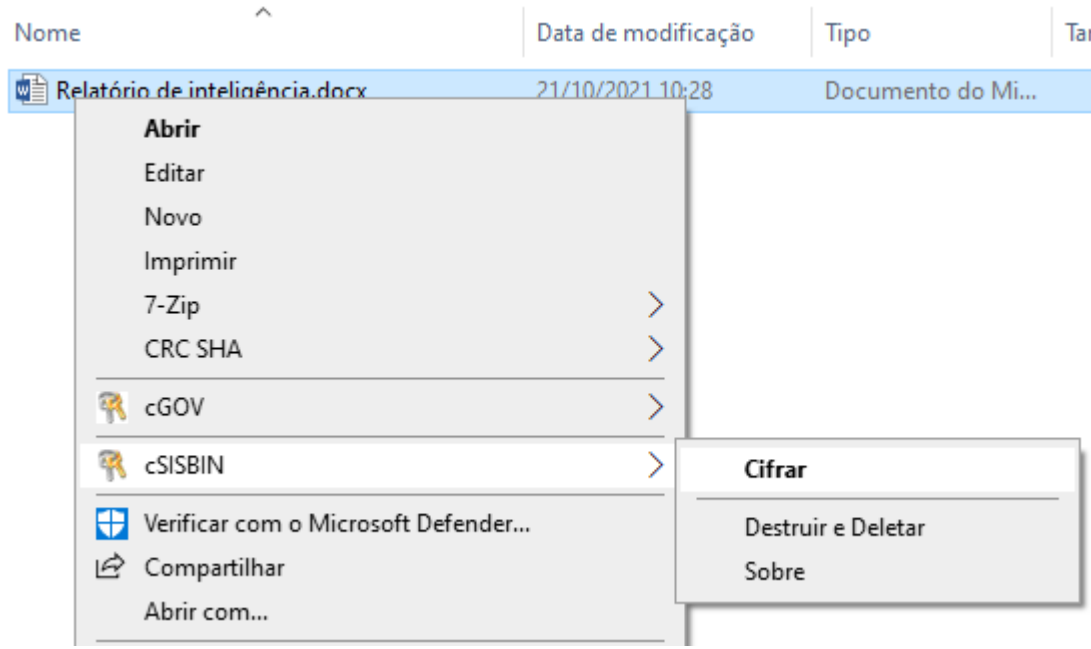
- Sistema operacional customizado
- Remoção de pacotes e serviços desnecessários
- Repositório próprio
- Regras de firewall
- Permissões de arquivos e pastas
- Grupos e usuários
- Cifração do disco
- Autenticação somente com PCP
- VPN somente com PCP
- Antivírus

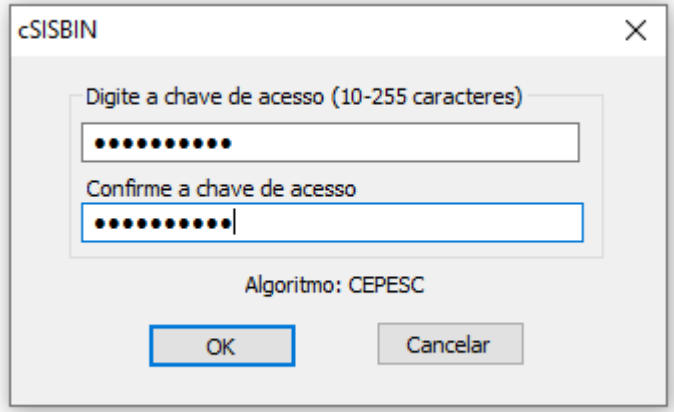
Agenda – Parte II

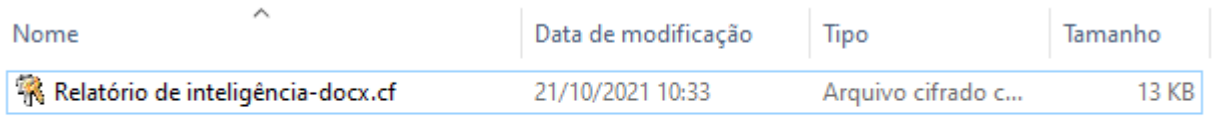
- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

cSisbin – Cifração de arquivos a partir de senha

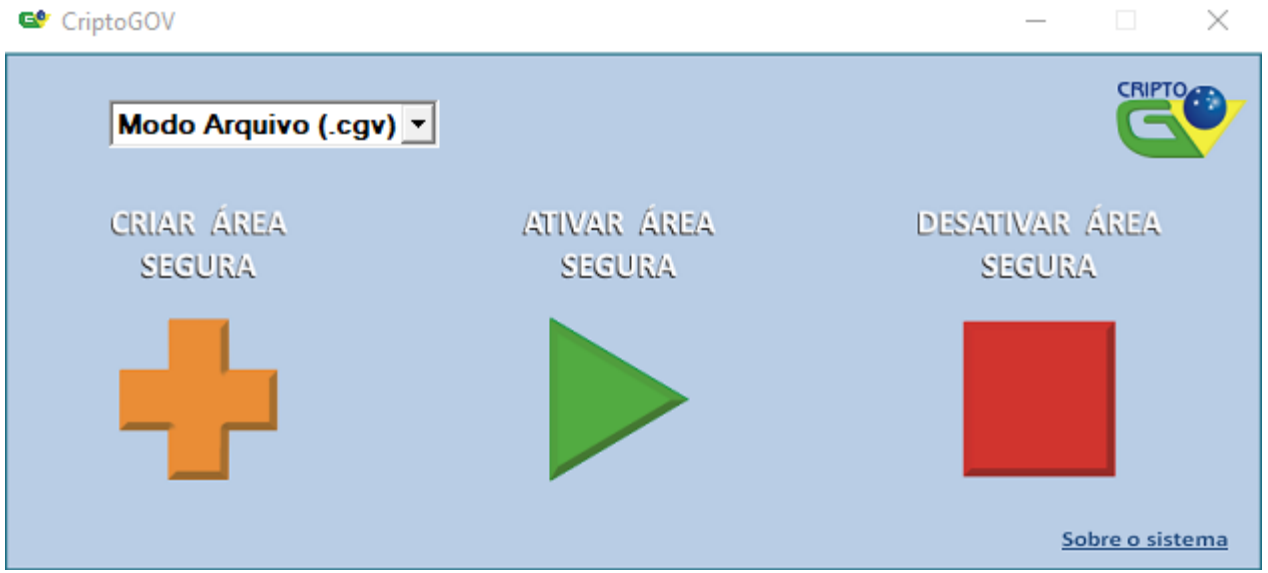






criptoGov – Criação de volumes seguros

- Armazenamento local seguro.
- Útil para o transporte seguro de muitos documentos em pendrive ou HD externo.

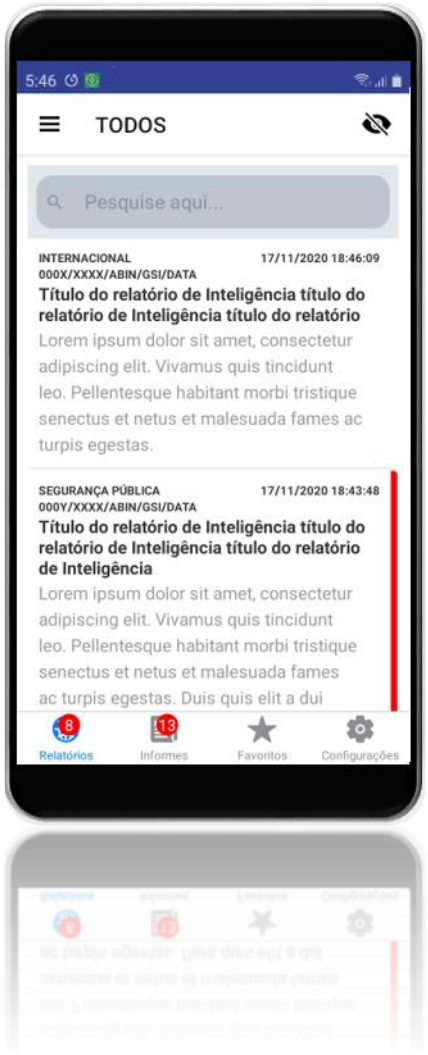


Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

RADAR



- Aplicativo para a difusão de informações de inteligência de forma rápida e segura.
- Faz a informação chegar nas mãos da autoridade final de forma imediata.

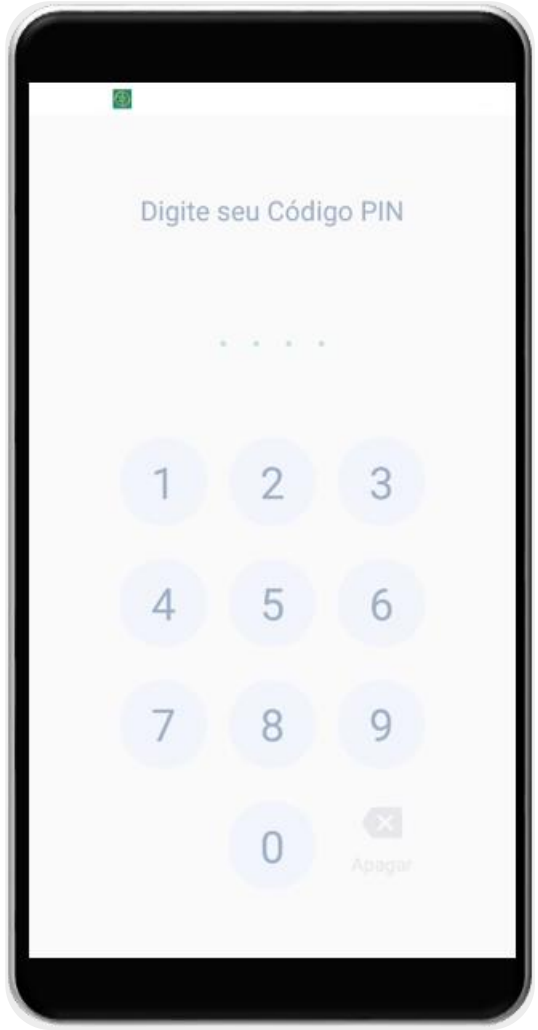
Feed de informações

ABIN

Grupos de difusão

ABIN

Segurança


Digite seu Código PIN
1 2 3
4 5 6
7 8 9
0
Apagar


5:21
Relatório
SECRETO
Briefing nº 0001/10974/ABIN/GSI/26 NOV. 2020
Impactos econômicos da construção do canal da Nicarágua
Em 22 dez. 2014, na cidade de Brito/Nicarágua, realizou-se cerimônia oficial de início das obras do Grande Canal Interoceânico da Nicarágua, que ligará os oceanos Atlântico e Pacífico por trajeto de 278 km no território nicaraguense. Além das eclusas, estão previstas a construção de dois portos, um oleoduto, uma ferrovia, duas zonas francas e um aeroporto internacional, infraestruturas de suporte, barragens, usinas para a geração de energia, indústria siderúrgica e de cimento e complexo turístico. As obras deverão estar concluídas até 2020.
Relatórios
Informes
Favoritos
Configurações

Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

ABIN

Previsão por lei

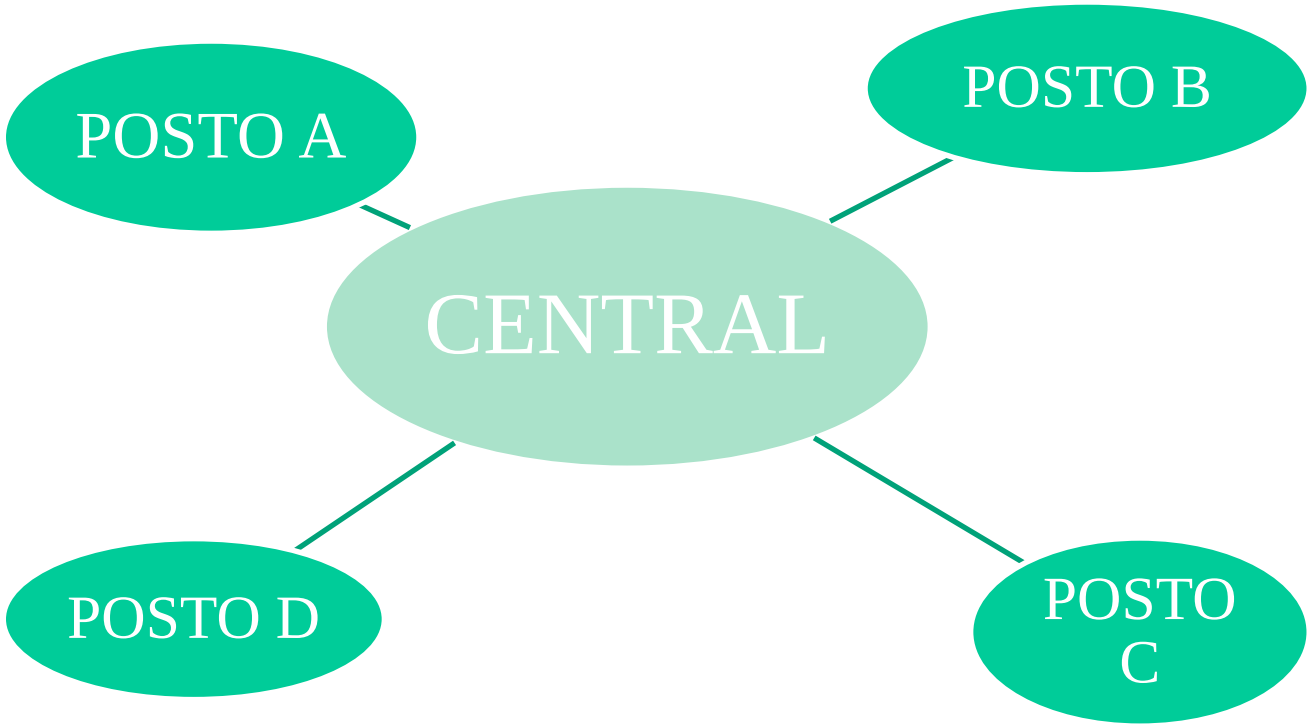
- A expedição, condução e entrega da informação classificada ultrassecreta (art. 27 decreto 7845) só pode ocorrer:
  - pessoalmente por agente público autorizado
  - por meio eletrônico, mediante uso de recursos criptográficos, conforme instrução normativa nº 3, do gsi/pr , de 6 de março de 2013:
    1. sistema de chave única
    2. algoritmo de sequência aleatória

Sistema de Sequências Aleatórias (SSA)

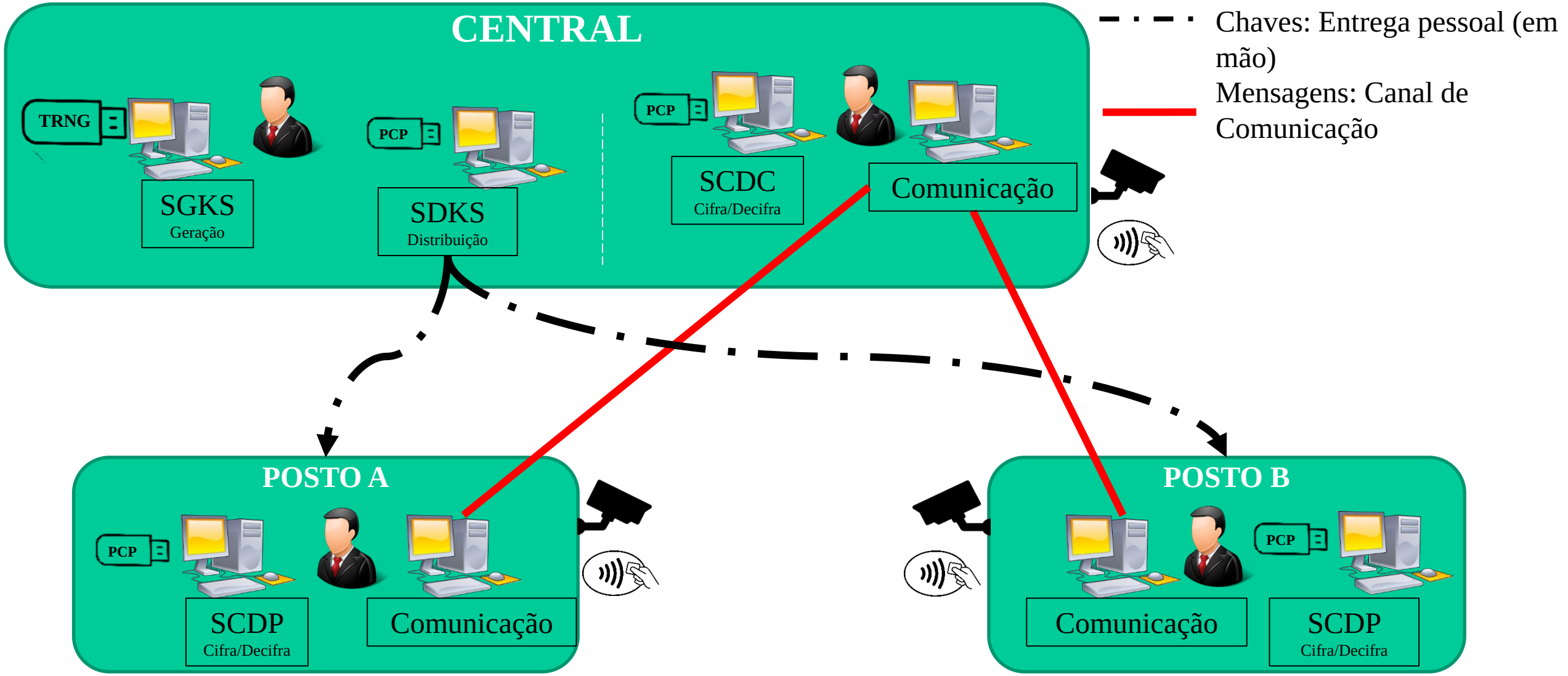
- Baseado em algoritmo de Estado.
- Sistema de chave única (cada chave é utilizada uma única vez);
- A chave é uma sequência aleatória; e
- A chave tem o mesmo tamanho da mensagem.

Sistema de Sequências Aleatórias (SSA)

- Arquitetura em estrela:
  - cada posto somente se comunica diretamente com a central
  - para um posto enviar uma mensagem a outro posto, deve fazer por meio da central



Sistema de Sequências Aleatórias (SSA)



Agenda – Parte II

- Solução de mensageria – Athena
- Criptografia em hardware – PCP e PCAD
- Solução de acesso remoto – Urutau
- Programas para cifração de arquivos e volumes – cSisbin e criptoGov
- Solução de difusão - Radar
- Sistema para criptografia de documentos Ultrassecretos – SSA
- Futuro – Criptografia de Estado como serviço

Criptografia de Estado como serviço

- Ou invés de fornecer produtos prontos, a ideia é o CEPESC oferecer serviços de criptografia de Estado que possam ser integrados nas soluções específicas de cada órgão.

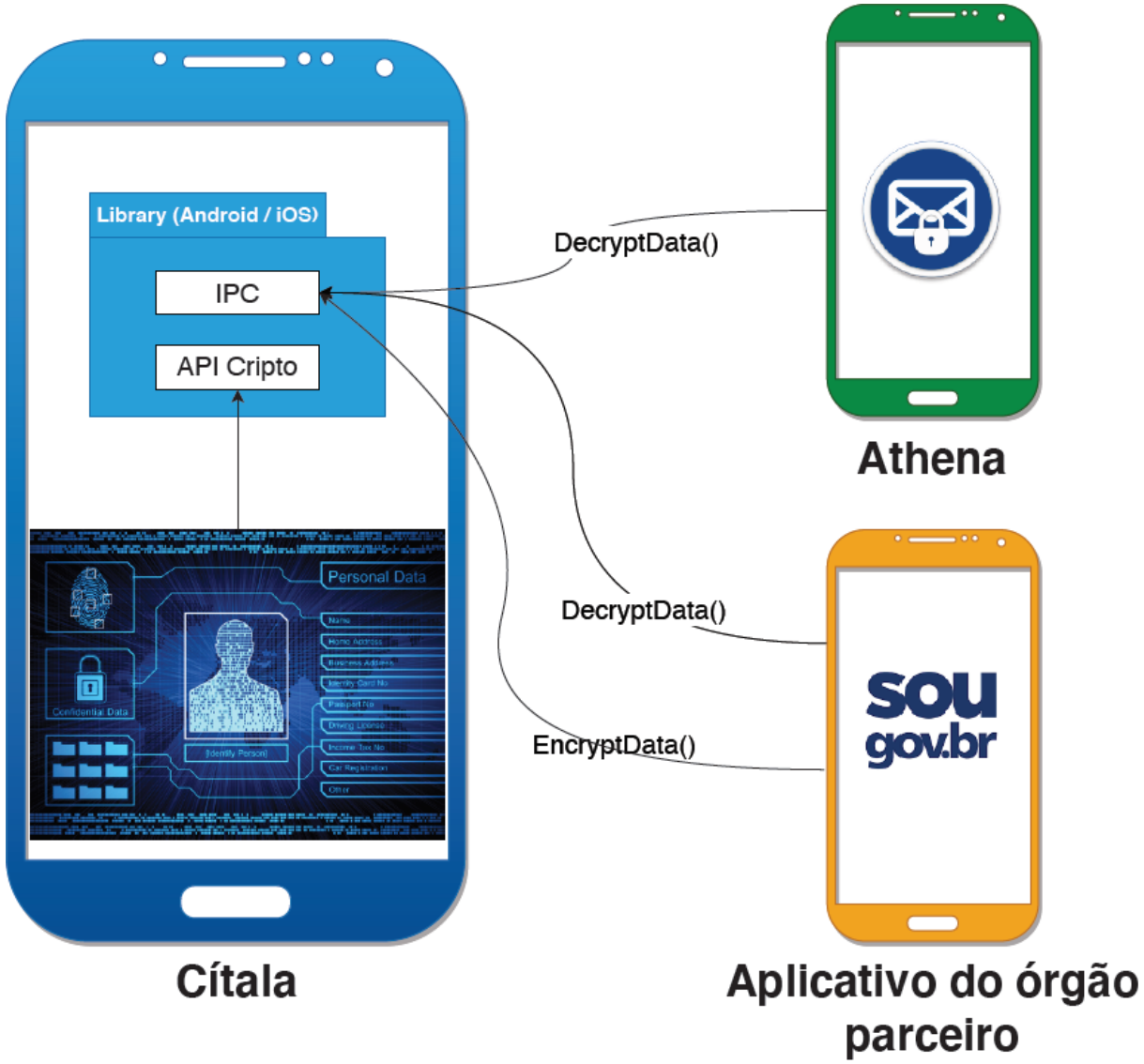
Criptografia de Estado como serviço

- Um exemplo é o projeto Arbor.
- Consiste em um serviço de certificação digital que possibilitará os servidores públicos possuírem uma Identidade Digital de Estado (IDE)

ABIN

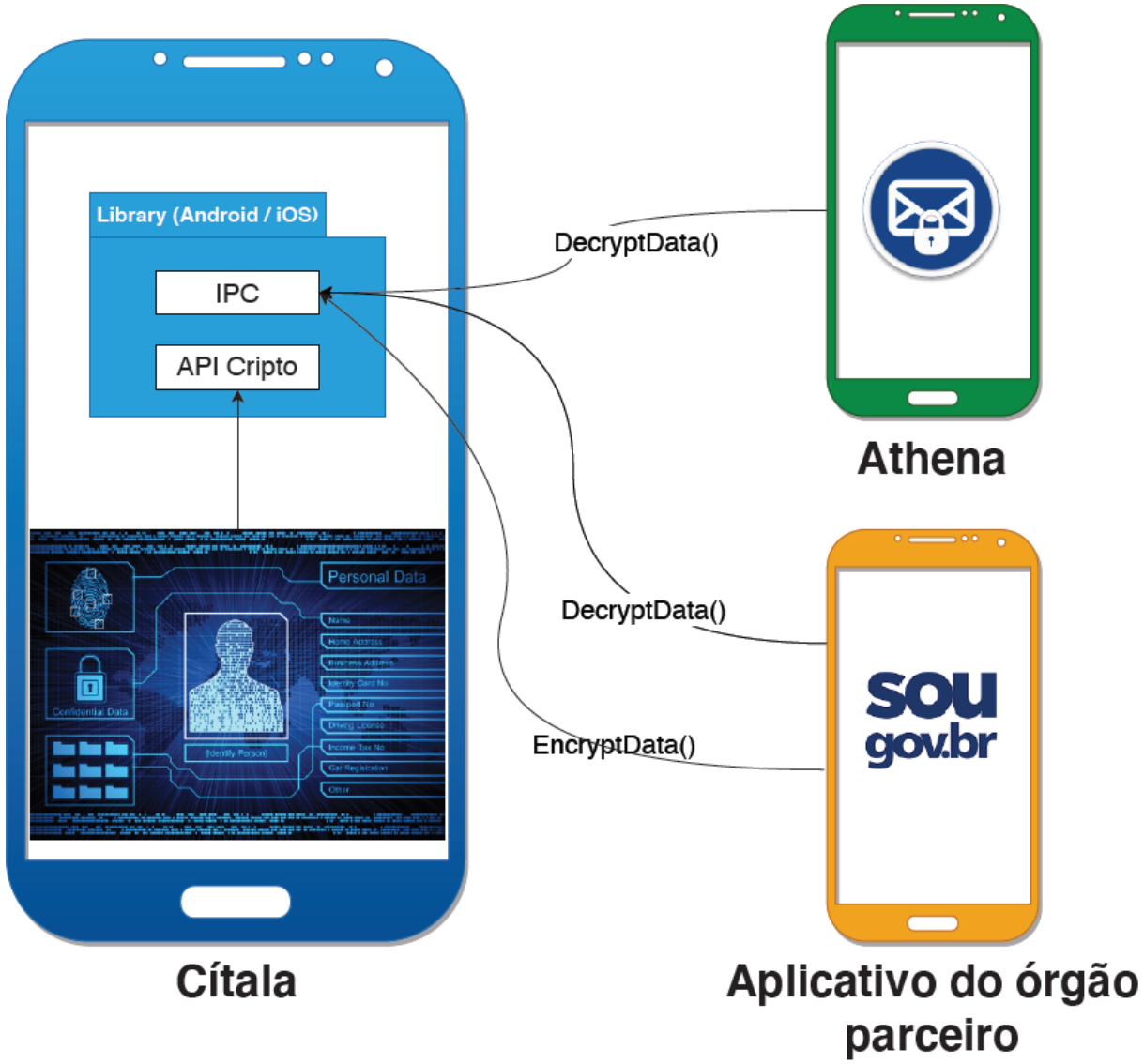
Criptografia de Estado como serviço

- Em combinação ao Arbor, está o aplicativo Cítala.
- O Cítala permite que aplicativos desenvolvidos por órgãos parceiros acessem a IDE e utilizem criptografia de Estado.



Criptografia de Estado como serviço

- Permite também criar um canal seguro entre aplicativos. Imagine, por exemplo, criptografar um arquivo sensível em seu aplicativo e encaminhar via Athena para um contato.



GABINETE DE
SEGURANÇA INSTITUCIONAL

PÁTRIA AMADA
BRASIL
GOVERNO FEDERAL