# Anexo X

Requisitos de Execução do Processo de Autenticação Bancária

**1. Escopo do Projeto NAI – Núcleo de Autenticação Interbancária**

***Dotar as aplicações do INSS de um sistema nacional de autenticação de usuários, baseado nos processos, bases cadastrais e bases documentais distribuídos nos Bancos Pagadores, permitindo ao Cidadão autenticar-se para acesso aos serviços da previdência social na internet utilizando-se de seus dados bancários.***

**2. Composição da Solução NAI – Núcleo de Autenticação Interbancária**

2.1. **Componente de Autenticação NAI** – Sistema provido pela plataforma NAI que oferece ambiente seguro de login e realiza ***autenticação de usuários*** para as aplicações do INSS. O Componente de Autenticação tem as seguintes Características:

2.1.1. Applet JAVA aberto em sessão SSL;

2.1.2. Função de criptografia de sigilo dos campos de dados de login e senha;

2.1.3. Dados de identificação do Usuário:

2.1.3.1. CPF

2.1.3.2. Banco – Lista de Bancos onde o Usuário indica o Banco com o qual tem vínculo;

2.1.4. Flexibilidade de emprego de diferentes chaves criptográficas, armazenadas em repositório específico;

2.1.5. A chave criptográfica usada na cifragem dos dados de login e senha será a do Banco com o qual o Usuário declara ter vínculo;

2.1.6. Dados de login cifrados pelo componente de autenticação com a chave criptográfica do Banco:

2.1.6.1. CPF do Usuário;

2.1.6.2. Agência;

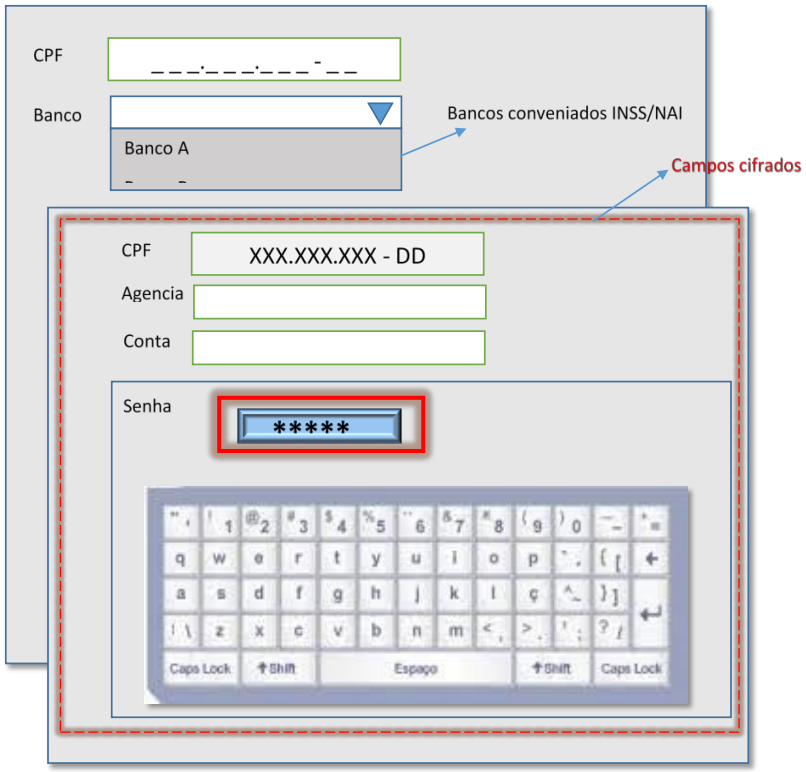
2.1.6.3. Número de Conta Corrente;

2.1.6.4. Senha bancária;

2.1.7. Envio do conjunto de dados de login e senha para o módulo Roteador de Transações de Autenticação conforme padrão e layout definidos;

2.1.8. Repasse do retorno da Transação de Autenticação, na forma de autenticação válida ou não-válida, para a aplicação INSS;

## Campos de autenticação




2.2. **Roteador de Transações de Autenticação – RTA** – Sistema provido pela plataforma NAI que submete a consulta de autenticação aos Bancos, conforme as seguintes macro funções:

2.2.1. Recebe do Componente de Autenticação a relação entre o CPF e o respectivo Banco indicado pelo Usuário;

2.2.2. Monta a Consulta de Autenticação com:

**2.2.2.1. Identificador da requisição**

**2.2.2.2. Dados cifrados:**

2.2.2.2.1. CPF

2.2.2.2.2. Agencia

2.2.2.2.3. Conta

2.2.2.2.4. Senha

2.2.3. Envia para o Banco através do canal seguro;

2.2.4. Recebe o resultado da Consulta de Autenticação enviada pelo Banco:

2.2.4.1. Identificador da requisição

2.2.4.2. Resultado da consulta: Autenticado ou Não-Autenticado (1 ou 0)

2.2.5. Armazena na base criptografada o conjunto de dados de identificação e o hash dos dados de autenticação:

**2.2.5.1. Dados de Identificação do Usuário**

2.2.5.1.1. CPF

2.2.5.1.2. Banco

**2.2.5.2. Dados de autenticação cifrados:**

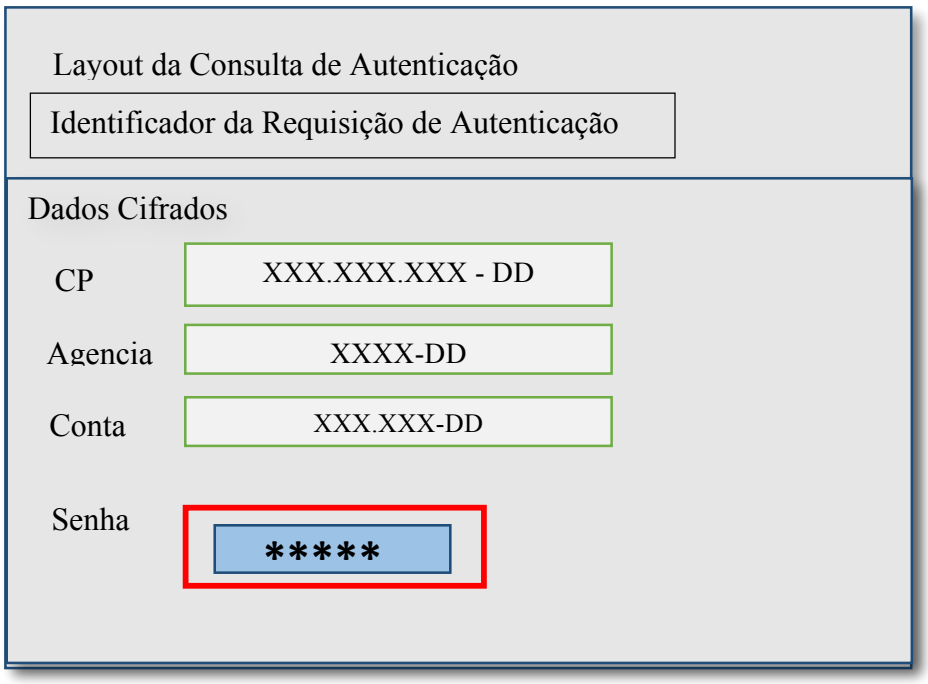
2.2.5.2.1. CPF

2.2.5.2.2. Agencia

2.2.5.2.3. Conta

2.2.5.2.4. Senha

2.2.6. Gera resultado da Consulta de Autenticação para a aplicação INSS;
2.2.7. Gera conjunto de elementos de rastreabilidade da transação de autenticação com timestamping padrão RFC 3161;




3. Requisitos para os bancos
   3.1. Insumos operacionais – Os Bancos deverão fornecer para a plataforma NAI:
      3.1.1. Fornecer e atualizar sua chave criptográfica pública e seu método de encriptação;
      3.1.2. Layout de formatação dos campos de Identificação: CPF, Agência e Conta-corrente
      3.1.3. Layout do campo Senha ATM
      3.1.4. Requisitos de conexão entre a sua estrutura e a plataforma NAI;

   3.2. Serviços de Autenticação executado pelo banco em seu próprio ambiente de alta segurança:
      3.3. Receber Consulta no layout definido através de conexão de dados segura;
      3.4. Decodificar os dados de identificação (CPF, Conta);
      3.5. Comparar senha;
      3.6. Gerar reposta à Consulta de Autenticação constituída de:
         3.6.1. Identificador da Requisição de Autenticação;
         3.6.2. Resultado da Consulta: Autenticado ou Não-Autenticado no padrão binário 1 ou 0