



MFA:

Um levantamento de métodos para autenticação com múltiplos fatores (Multi-factor Authentication)

Dayana Spagnuolo

Universidade Federal de Santa Catarina

Jeroen van de Graaf

Universidade Federal de Minas Gerais

Sumário



- Introdução
- Autenticação eletrônica
- Guia de autenticação eletrônica
- Métodos de Autenticação
- Cenário de uso

Introdução



- Ampla utilização de usuário e senha
- Modelo não mais suficiente
- Vulnerabilidades com proporções maiores
- Necessidade de novos métodos

Introdução



- Alternativas mais seguras
- Não somente mais seguras, mas também:
 - de baixo custo
 - de fácil implementação
 - de boa aceitação
- Levantamento de métodos de autenticação!

Autenticação eletrônica



- "Processo de estabelecer confiança em identidades apresentadas eletronicamente"
- Registro
 - Prova de identidade
 - Cadastro de informações
 - Acordo de segredos
- Autenticação
 - Apresentação e verificação de credenciais
 - Fatores de autenticação

Autenticação eletrônica



- Fatores:

- Algo que se sabe



Autenticação eletrônica



- Fatores:

- Algo que se sabe
- Algo que se possui



Autenticação eletrônica



- Fatores:

- Algo que se sabe
- Algo que se possui
- Algo que se é



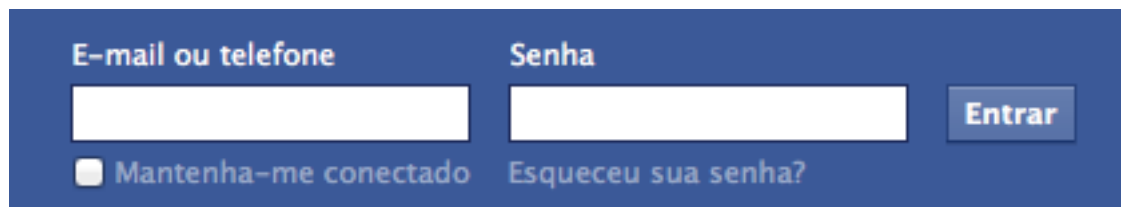
Autenticação eletrônica



- Um ou mais fatores por autenticação

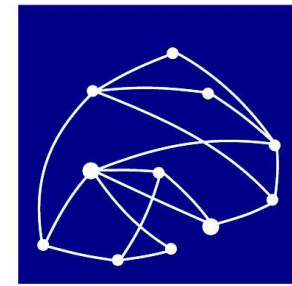


Algo que se sabe +
Algo que se possui

A screenshot of the Facebook login interface. It features a blue header bar with the text 'E-mail ou telefone' and 'Senha' above two white input fields. To the right of the password field is a blue 'Entrar' button. Below the input fields, there is a checkbox labeled 'Mantenha-me conectado' and a link that says 'Esqueceu sua senha?'.

Algo que se sabe

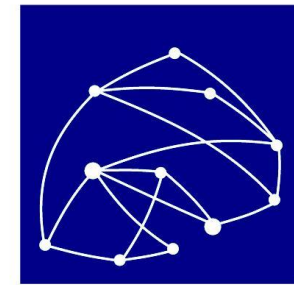
Guia de autenticação eletrônica



RNP

- Criado pelo Instituto Nacional de Padrões e Tecnologia (NIST) dos Estados Unidos
- Versão 800-63-1 lançada em Dezembro de 2011
- Recomendações para autenticações remotas
- Auxilia na escolha de tecnologias que satisfaçam o nível de segurança requerido
- Define 4 níveis (1 é o mais baixo, 4 o mais alto)

Guia de autenticação eletrônica



RNP

- Divide a autenticação em 5 áreas
 - Registro e prova de identidade
 - Tokens
 - Gerenciamento de tokens e credenciais
 - Protocolos
 - Mecanismos de asserção

Métodos de autenticação



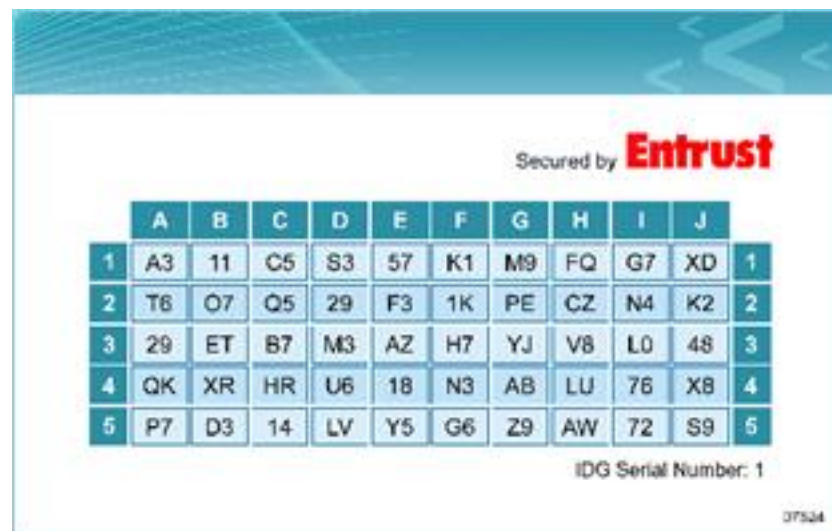
- Usuário e senha
 - PIN
 - Pass Phrase
 - Fast word
 - Senhas randômicas

- Perguntas de cunho pessoal

Métodos de autenticação



- Lista de senhas únicas
- Grid Card

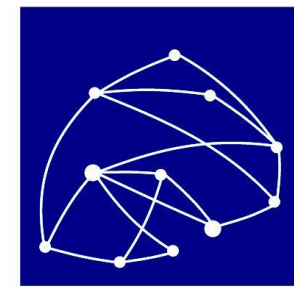


Métodos de autenticação

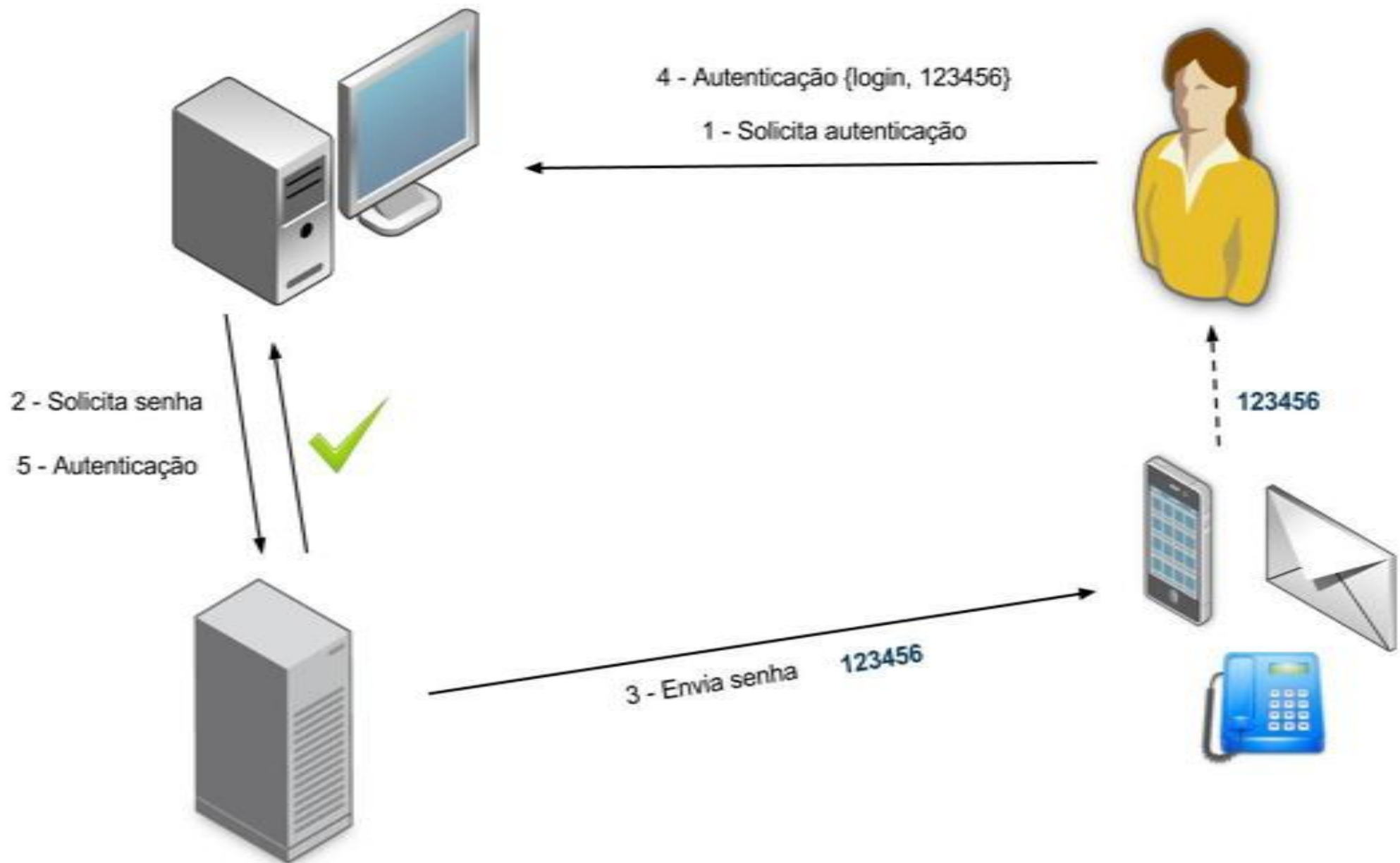


- Contrassenha
 - SMS
 - Telefonema
 - E-mail

Métodos de autenticação



RNP

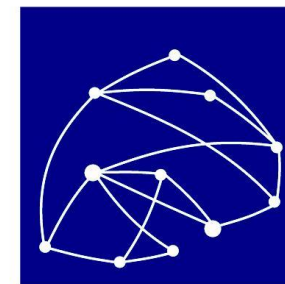


Métodos de autenticação

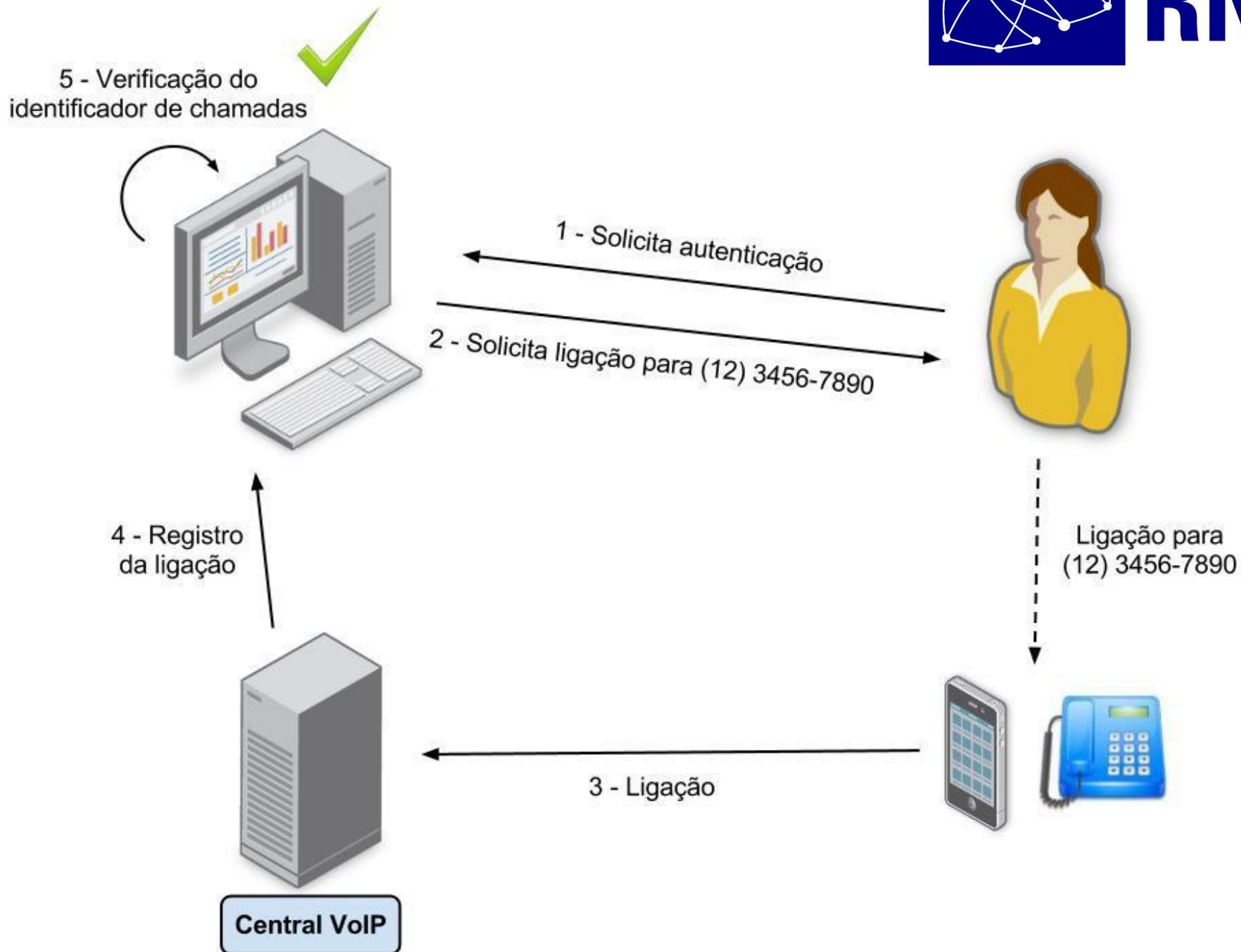


- Identificação de chamadas

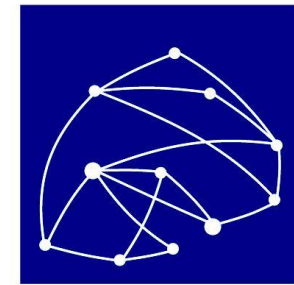
Métodos de autenticação



RNP



Métodos de autenticação



RNP

- One-Time Password
 - Google Authenticator
 - Hardware dedicado



Métodos de autenticação



- Tigr

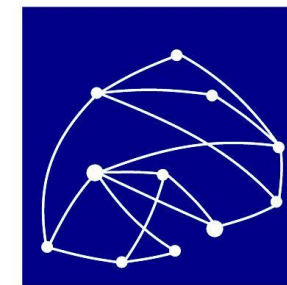


Métodos de autenticação



- Desafio Resposta - Chave assimétrica
- Pico
- Biometria

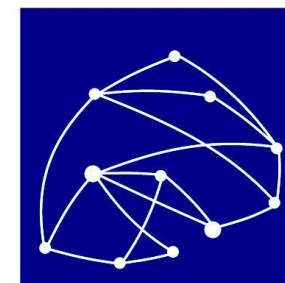
Métodos de autenticação



RNP

Método	Nível	Requisitos Específicos	Requisitos comuns
Usuário e senha	1	6 caracteres	Limitar as tentativas falhas a 100 por mês, com verificações mais frequentes (diárias)
	2	8 caracteres	
PIN	1	4 dígitos aleatórios, ou 10 escolhidos pelo usuário	
	2	6 dígitos aleatórios, ou 15 escolhidos pelo usuário	
Pass-Phrase	2	8 caracteres	
Fast word	1	6 caracteres	
	2	8 caracteres	
Senha randômica	2	4 caracteres	
Perguntas de cunho pessoal	1	5 perguntas	
	2	7 perguntas	
Lista de senhas únicas	2	6 dígitos ou 4 caracteres	-
		20 dígitos ou 10 caracteres	

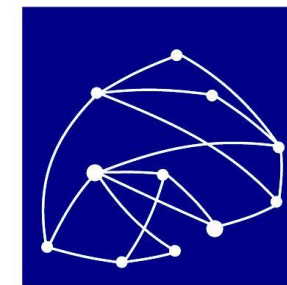
Métodos de autenticação



RNP

Método	Nível	Requisitos Específicos	Requisitos comuns
Desafio resposta - Grid Card	1	4 dígitos	Limitar as tentativas falhas a 100 por mês, com verificações mais frequentes (diárias)
	2	6 dígitos	
Contrassenha - SMS	2	6 dígitos ou 4 caracteres	
		20 dígitos ou 10 caracteres	-
Contrassenha - Telefonema	2	20 dígitos ou 10 caracteres	-
		6 dígitos ou 4 caracteres	Limitar as tentativas falhas a 100 por mês, com verificações mais frequentes (diárias)
Contrassenha - e-mail	-	-	-
Identificação de chamadas	-	-	-

Métodos de autenticação



RNP

Método	Nível	Requisitos Específicos	Requisitos comuns
OTP - Google Authenticator	2	Servidor de autenticação validado em FIPS 140-2 nível 1	Tempo de vida das senhas na ordem de minutos
OTP - Hardware	4	Hardware validado em FIPS 140-2 nível 2 ou mais, com segurança física FIPS 140-2 nível 3 ou mais	
		Tempo de vida das senhas com menos de 2 minutos	
Tiqr	3	Validação FIPS 140-2 nível 1 ou mais	Desafio com 20 dígitos ou 10 caracteres
Desafio resposta - Chaves assimétricas	2	Validação FIPS 140-2 nível 1 ou mais	
	4	Validação FIPS 140-2 nível 2 ou mais, com segurança FIPS 140-2 nível 3 ou mais	
Pico	-	-	-
Biometria	-	-	-

Cenário de uso

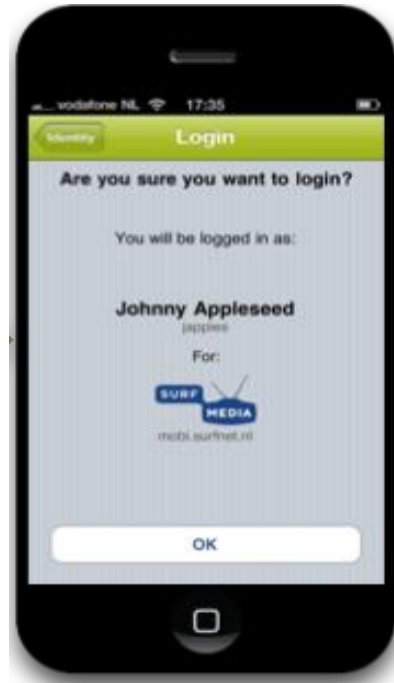


- Supondo um cenário onde um sistema web necessita de uma autenticação forte (aprox. nível 3 ou mais) sem a introdução de nenhuma nova infra-estrutura física. Qual método utilizar?

Cenário de uso



- Supondo um cenário onde um sistema web necessita de uma autenticação forte (aprox. nível 3 ou mais) sem a introdução de nenhuma nova infra-estrutura física. Qual método utilizar?



tiqr

Nível de garantia - 3

Criptografia simétrica

Multi-factor cryptographic device

Cenário de uso



- Supondo um cenário onde um sistema web necessita de uma autenticação forte (aprox. nível 3 ou mais) sem a introdução de nenhuma nova infra-estrutura física. Alternativas?

Cenário de uso



- Supondo um cenário onde um sistema web necessita de uma autenticação forte (aprox. nível 3 ou mais) sem a introdução de nenhuma nova infra-estrutura física. Alternativas?



Google Authenticator

Nível de garantia - 2

PIN para desbloqueio de celulares

Quase MF OTP Device (nível 3)

Cenário de uso



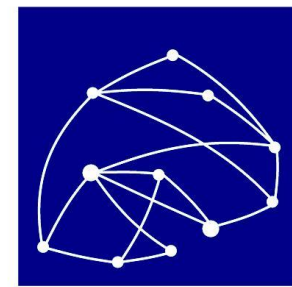
- Supondo um cenário onde um sistema web necessita de uma autenticação forte (aprox. nível 3 ou mais) sem a introdução de nenhuma nova infra-estrutura física. Alternativas?



Contrassenha via SMS

Nível de garantia - 2

PIN para desbloqueio de celulares
Out of band



RNP

Perguntas?

Dayana Spagnuolo
dayspagnuolo@inf.ufsc.br

Jeroen van de Graaf
jvdg@dcc.ufmg.br