augmented security

Solution Universelle d'Authentification Forte

Sobre o que estamos tomando

O crime cibernético custa à economia global US$1.000 bilhões por ano, metade do valor de dois anos atrás!

Entre resgates e hacking, o crime cibernético procura diversificar

Existem obrigações legais

Diretiva de Serviços de Pagamento 2

Normas de segurança mais rígidas para pagamentos on-line para aumentar a confiança dos consumidores nas compras on-line.

Forte autenticação

A autenticação forte, ou autenticação de dois fatores, combina o uso de dois elementos de três categorias: algo que você sabe (senha, código PIN), algo que você tem (computador, telefone celular), algo que você é (impressão digital, retina, voz).

Qual é nosso ponto forte

Em um mundo onde nossos dados (profissionais e pessoais) valem seu peso em ouro

- Acesso por simples "Login/Password" é ilegal para qualquer compra
- Aumento do hacking
- Desenvolvimento do comércio eletrônico
- Muitas senhas diferentes desaceleram as operações e criam abandono de compras
- O SMS é facilmente hackeável

A Segurança Aumentada foi premiada com uma patente européia
Demonstrar isso é uma solução forte, única e simples.

Fase de inscrição 1

PRELIMINÁRIO

- Baixe o aplicativo IOS ou Android
- Preencher os dados pessoais
- Funciona em qualquer smartphone ... qualquer IOT ou PC's

01

Digite suas informações de login

02

Digite a chave de ativação

Fase de inscrição 2

03

Digite seu código secreto

04

Pronto para uso

Modo de autenticação

01

IDENTIFICAÇÃO

pela posse de seu dispositivo

02

SELF-IDENTITY

por seu código secreto

03

AUTENTICAÇÃO SUCESSÍVEL

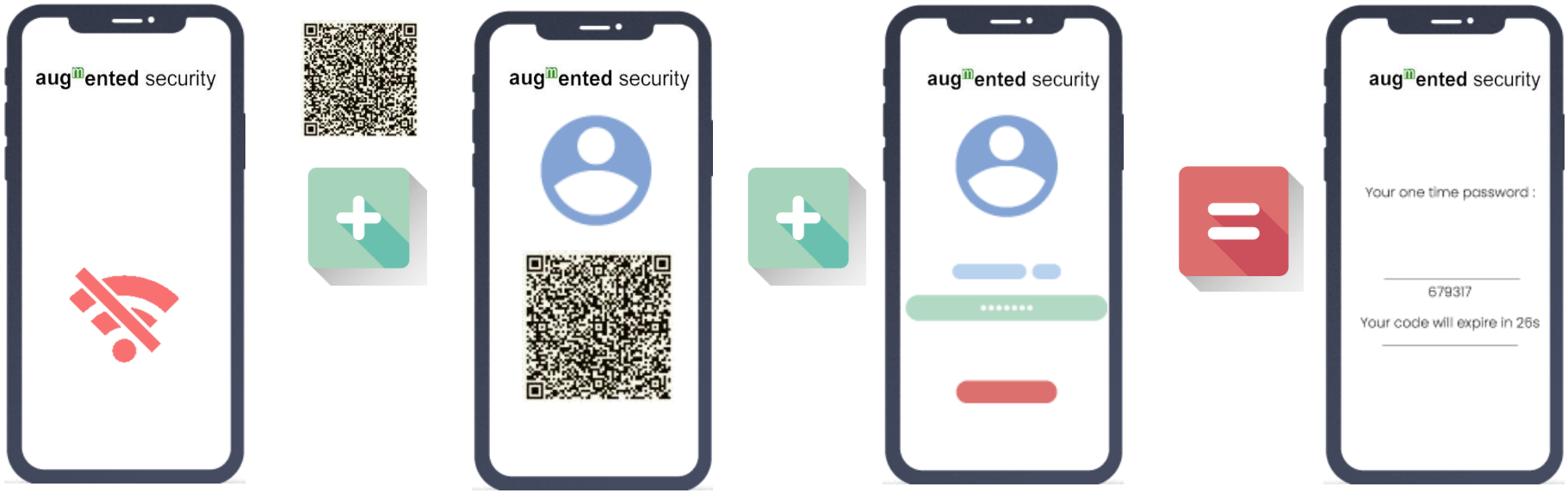
Modo de autenticação desconectado

01
Lançamento do aplicativo

02
Digitalização do Código QR

03
Inserindo o código PIN

04
OTP Gerado



Benefícios para o usuário

Proteção da identidade do usuário

- Dados do usuário armazenados em formato criptografado no servidor de autenticação servidor de autenticação (processamento criptográfico)

Aplicação segura para smartphone

- Nenhum dado armazenado pelo aplicativo para smartphone
- Código totalmente "ofendido" (chamadas de sistema ocultas...)

Facilidade de uso

- Viagem instintiva do cliente
  Validação através de um simples código PIN escolhido pelo cliente.
- Nenhuma informação armazenada no smartphone.
- Se o telefone for perdido/roubado, mesmo se estiver desbloqueado
  a aplicação é inutilizável
  solução independente de cartão SIM e terminal

racterísticas de alta segurança

Autenticação forte de 2 fatores patenteada

- Assinatura do hardware do smartphone (número de série do processador...) ou equivalente
- **Código pessoal definido pelo usuário durante a matrícula. Sempre o mesmo**

3 níveis de resistência aos ataques do "Homem no Meio".

- Smartphone - Link de servidor de autenticação realizado em HTTPS/TLS V1.2
- Criptografia de todos os dados trocados por chave de sessão AES
- Criptografia excessiva de dados sensíveis (SHA2, Bcrypt)

Resistência à Phishing

- Chave de sessão AES enviada pela aplicação smartphone criptografada pela chave pública do servidor de autenticação
- Certificado de autenticação do servidor verificado pelo aplicativo smartphone
- Chave exclusiva pública/privada para cada servidor de autenticação
- Suporte ao protocolo SAML para autenticação de Single Sign On (SSO)

poucas palavras

01	**Simplificação do PSD2:** senha do usuário utilizada, não a enviada pelo fornecedor.
02	**Código pessoal** definido pelo usuário durante a matrícula.
03	**Patente européia**, know-how francês

Mercado automotivo & mais

Órgãos públicos


e-universidade


e-administração


e-saúde

e-vote

Empresas


Acesso à rede/web


Acesso físico


Ciber-segurança


Varejo


Transporte


Redes sociais

Bancos


Home banking


Saque em dinheiro


Transferência de dinheir


M-pagamento


comércio eletrônico

augmented security

Solution Universelle d'Authentification Forte

Jacques PAUCKER
Presidente
jacques.paucker@augmented-security.net
+33 (0)6 86 13 10 26

Charles ORSEL des SAGETS
Parceiro, responsável pelo desenvolvimento dos negócios
charles.orseldessagets@augmented-security.net
+33 (0)6 72 86 71 90

Embargo ao comunicado de

Jacques Paucker assume a **Segurança Aumentada** e anuncia que sua forte solução de autenticação simplifica o processo de validação enquanto atende ao padrão **DSP2.**

Sua patente torna possível proteger e proteger os veículos conectados contra penetração criminosa, evitando a necessidade de receber um novo código a cada checkout.
O especialista em automóveis Jacques Paucker foi presidente da Logikko, empresa que ele co-fundou em 2013, até março de 2021.

Esta empresa, na qual permanece acionista, é um participante comprometido na transição ecológica, desenvolvendo uma tecnologia patenteada baseada na injeção de hidrogênio para melhorar a combustão em motores de combustão e reduzir drasticamente sua poluição.

Embargo ao comunicado de

Hoje, outro campo fundamental está aberto para inovações revolucionárias: Segurança M2M entre um motor e a Internet. De fato, estas transações não são seguras, o que permite, por exemplo, assumir o controle total ou parcial de um motor de carro, ônibus, caminhão ou barco....

Hoje, a **Segurança Aumentada** é uma verdadeira tecnologia disruptiva baseada na assinatura do material do componente de comunicação do proprietário de um veículo.
Jacques **Paucker** explica: "*No mundo do veículo conectado, graves problemas de segurança cibernética surgem. A Segurança Aumentada oferece a garantia de um nível superior de segurança para todo o acesso aos dados do veículo e do usuário.* "