ibs info
business solutions
integradora de sistemas

We are the new secure communication mindset

SIKUR ID

NOSSOS CONTATOS

Para saber mais sobre adesão, entre em contato com nossa equipe comercial:

marcos.damiao@ibs1.com.br

andree.miranda@ibs1.com.br

comercial@ibs1.com.br

Telefone / Fax
55 21 2233-5374 - 21 2256-4552
21 3178-4110

Cel. WhatsApp:
21 99904-4974
21 97168-5754

O tamanho do mercado de cibersegurança

Em 2004, o mercado global de cibersegurança valia **US$ 3,5 bilhões** — e em 2017 valia mais de **US$ 120 bilhões**. O mercado de cibersegurança cresceu cerca de **35X durante esse período de 13 anos** — antes do último dimensionamento de mercado pela Cybersecurity Ventures, para o período de 5 anos de 2017 a 2021.

Source: Cybercrime Magazine, 2020

Hacker vaza senhas para mais de 5000.000 servidores, roteadores e dispositivos IoT

Source: ZDNet, 2020

Apesar das promessas de desenvolvedores de biometria e reconhecimento facial de um futuro sem mais senhas — o que pode, de fato, acontecer em um ponto no futuro distante —, um relatório conclui que o mundo precisará proteger globalmente 300 bilhões de senhas globalmente até 2020..

Source: Cybercrime Magazine, 2020

63% de violações de dados confirmadas envolveram senhas fracas, padrão ou roubadas.

Source: Verizon Data Breach Report, 2016

A criptografia é um padrão agora, e em breve outros controles de segurança surgirão como requisitos rígidos nos termos do artigo 32° GDPR, como a autenticação multifatorial [MFA] ao processar dados pessoais de maior risco.

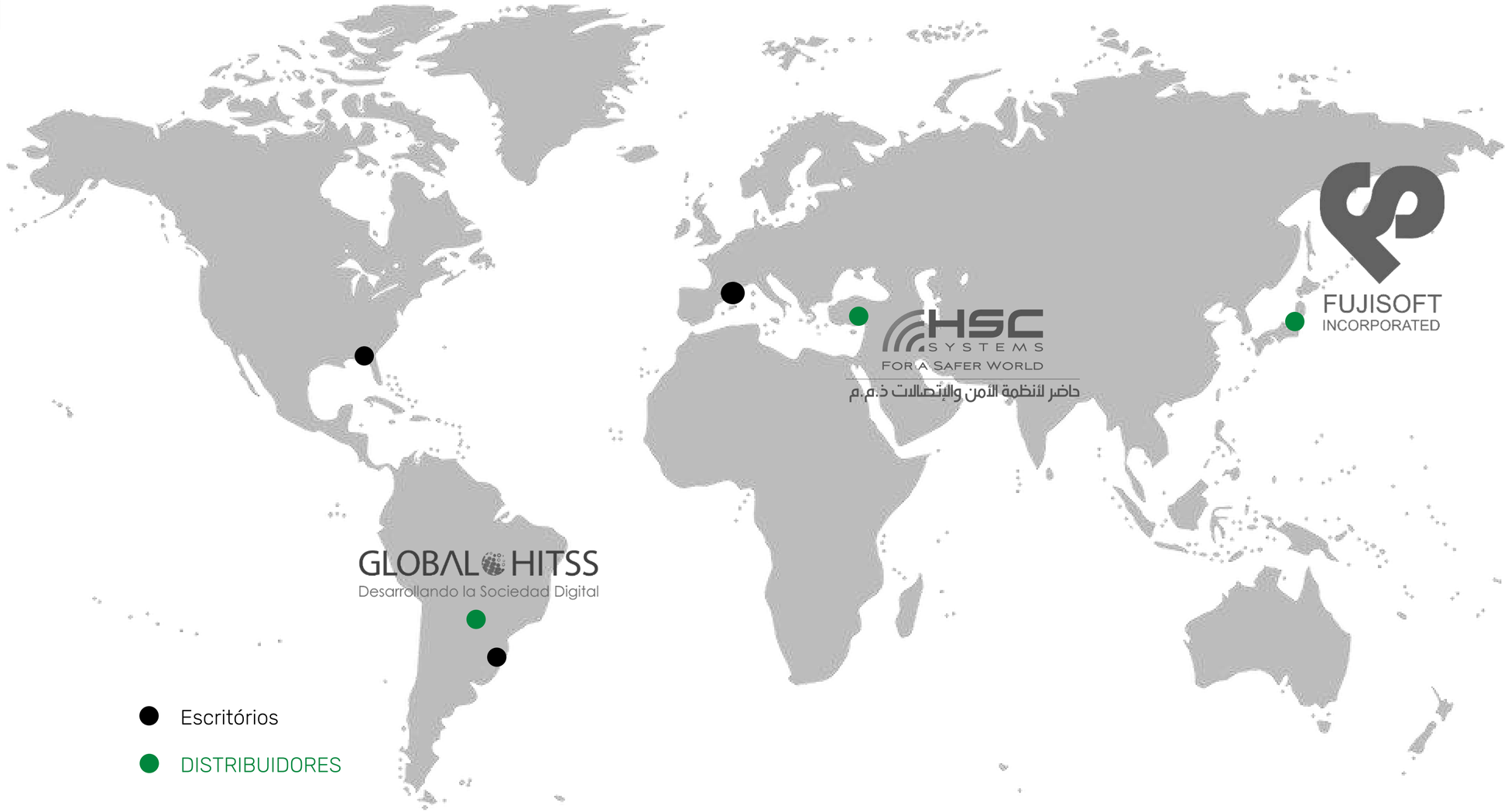
Source: Computer Weekly

CEOs, diretores de conselhos e investidores institucionais consideram a segurança cibernética nacional e corporativa uma ameaça ao crescimento dos negócios e a economia global.

Source: EY

A Companhia

A Sikur está definindo o futuro da comunicação segura, operando globalmente, através de seus escritórios e distribuidores no Brasil, Estados Unidos, Europa, Oriente Médio e Japão. Sikur trabalha ao lado de governos e corporações que acreditam que a segurança é fundamental para a integridade de seu trabalho. Acreditamos que a segurança não se trata apenas de plataformas e sistemas digitais, mas é uma mentalidade que envolve todos os aspectos de um negócio.



O Sikur Lab é o novo laboratório de inovação e pesquisa sikur localizado em Sophia Antipolis, França. Sikur é membro do setor de Segurança Digital do Sophia Antipolis SCS Cluster (Secure Communicating Solutions), que é um ecossistema europeu líder em microeletrônica, internet das coisas, segurança digital, inteligência artificial e big data. Estabelecemos nosso laboratório de pesquisa neste local porque é um hub de rápido crescimento em tecnologias avançadas. Agora, a digitalização é o cerne de tudo relacionado ao desenvolvimento humano, e a França está ocupando um papel central como temos notado nos últimos anos. Isso está acontecendo em paralelo com o desenvolvimento da Sikur como empresa, e queremos participar disso, no mesmo ritmo rápido.

Exposição Global

SIKUR: “ONE OF THE MOST EXCITING PHONES AND GADGETS FROM MWC 2018”

WIRED

Gartner

According to Gartner, SIKUR is a vendor that has relevant solutions to this technological space

hackerone

Pushing its technology to the limit, SIKUR launched the safest smartphone ever in 2016. Not satisfied delivered it to the world best hackers, and gave them a mission: break it. They failed.

Mashable

c|net

Forbes

WSJ

TechCrunch

CNBC

engadget

CNN

REUTERS®

Bloomberg

Fundação Segura – H2H/ H2M/ H2M2M

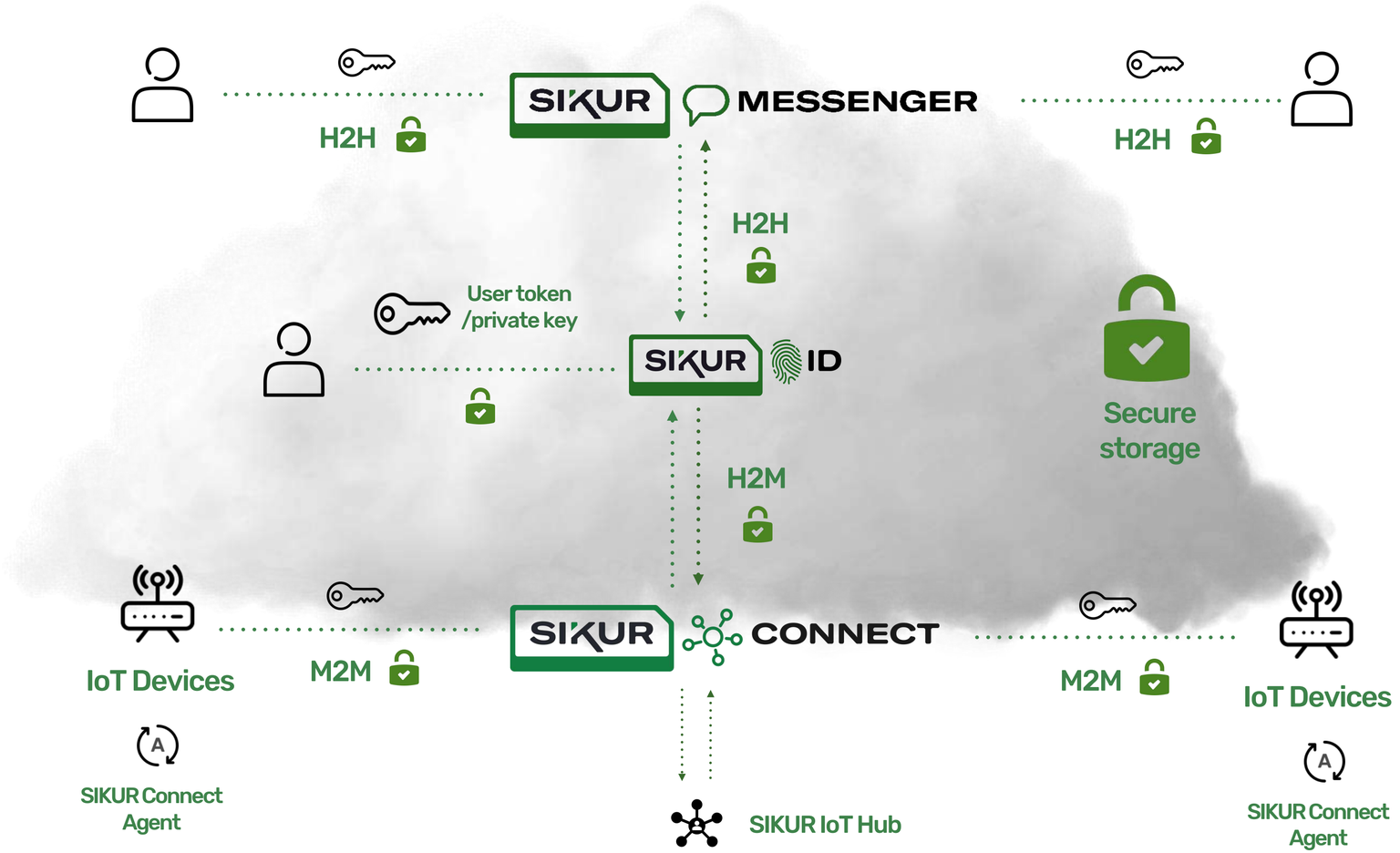
Nuvem

APPs

Endpoints

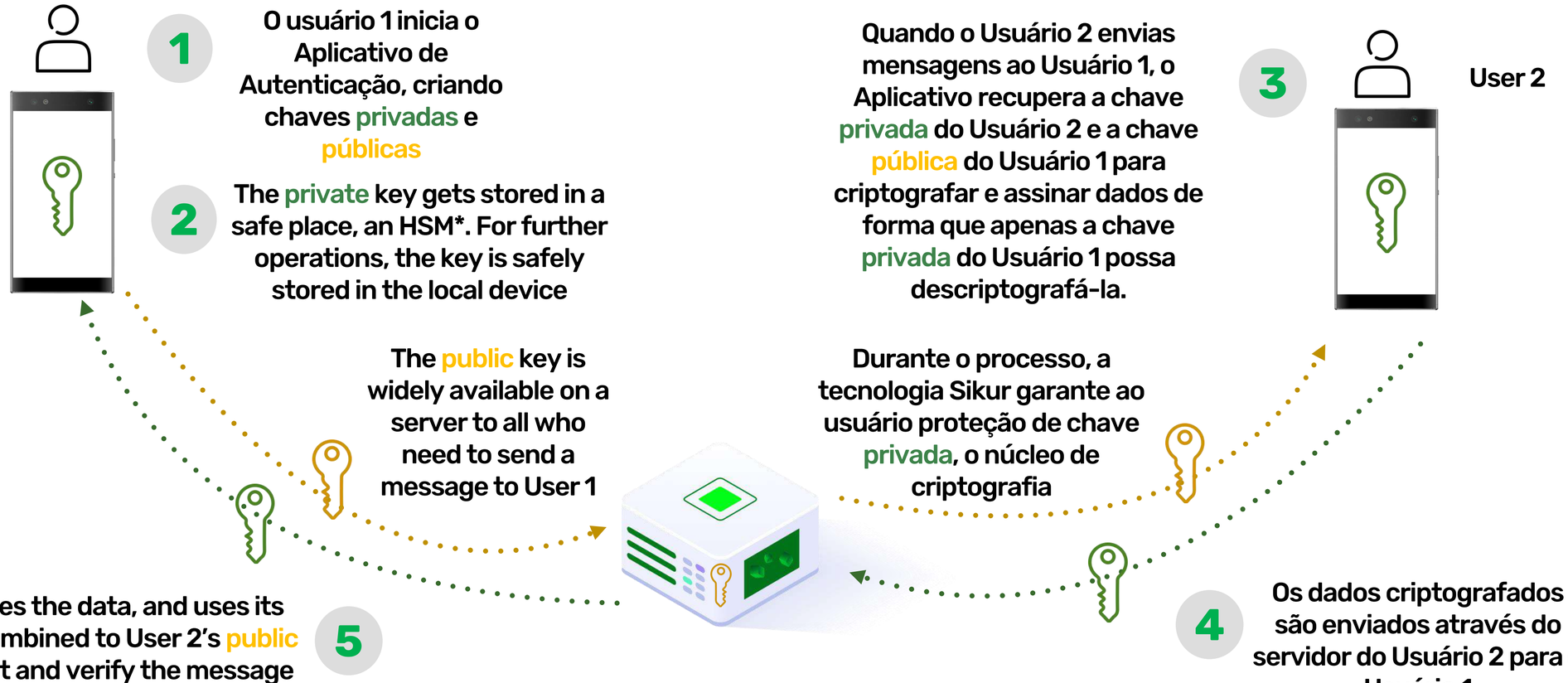
Solução de Comunicação Encapsulada

1. autenticação forte
2. não-repúdio
3. armazenamento seguro
4. comunicação segura



Como funciona: Chave privada Sikur ID

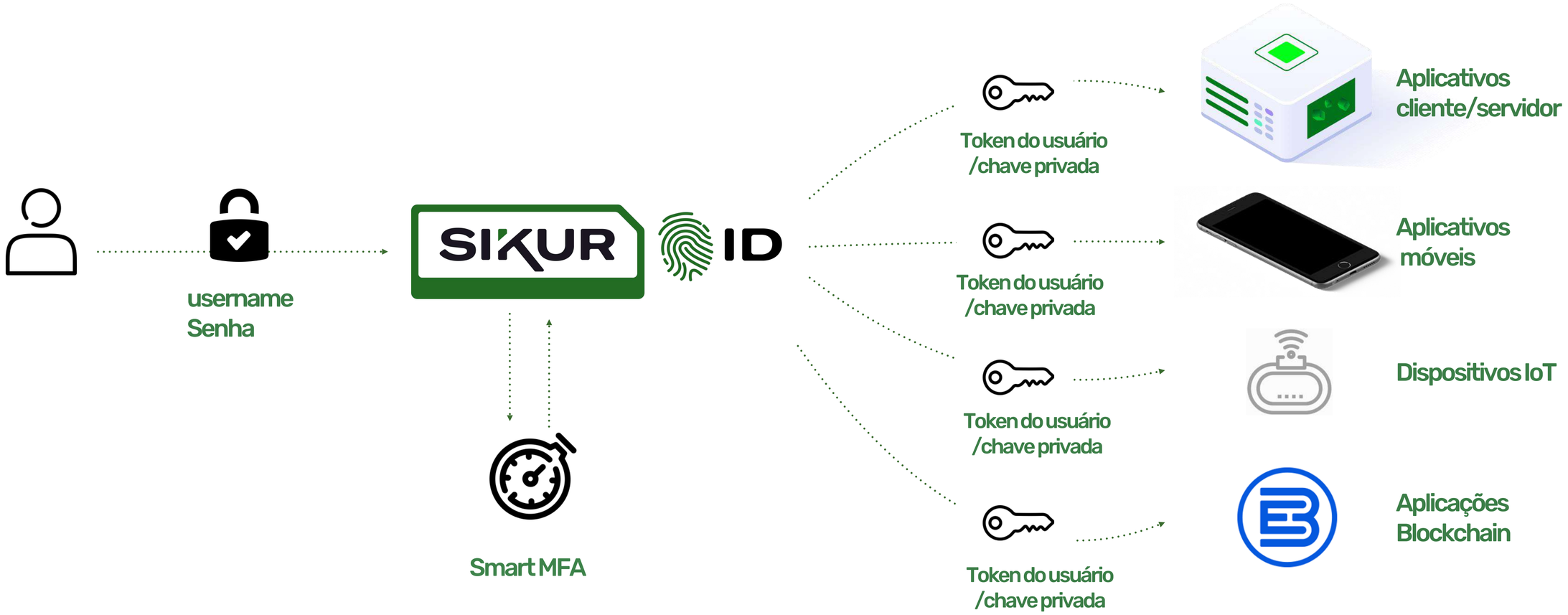
Quebrar a criptografia significa descobrir ambas as chaves. Usando força bruta, leva décadas com os computadores de hoje



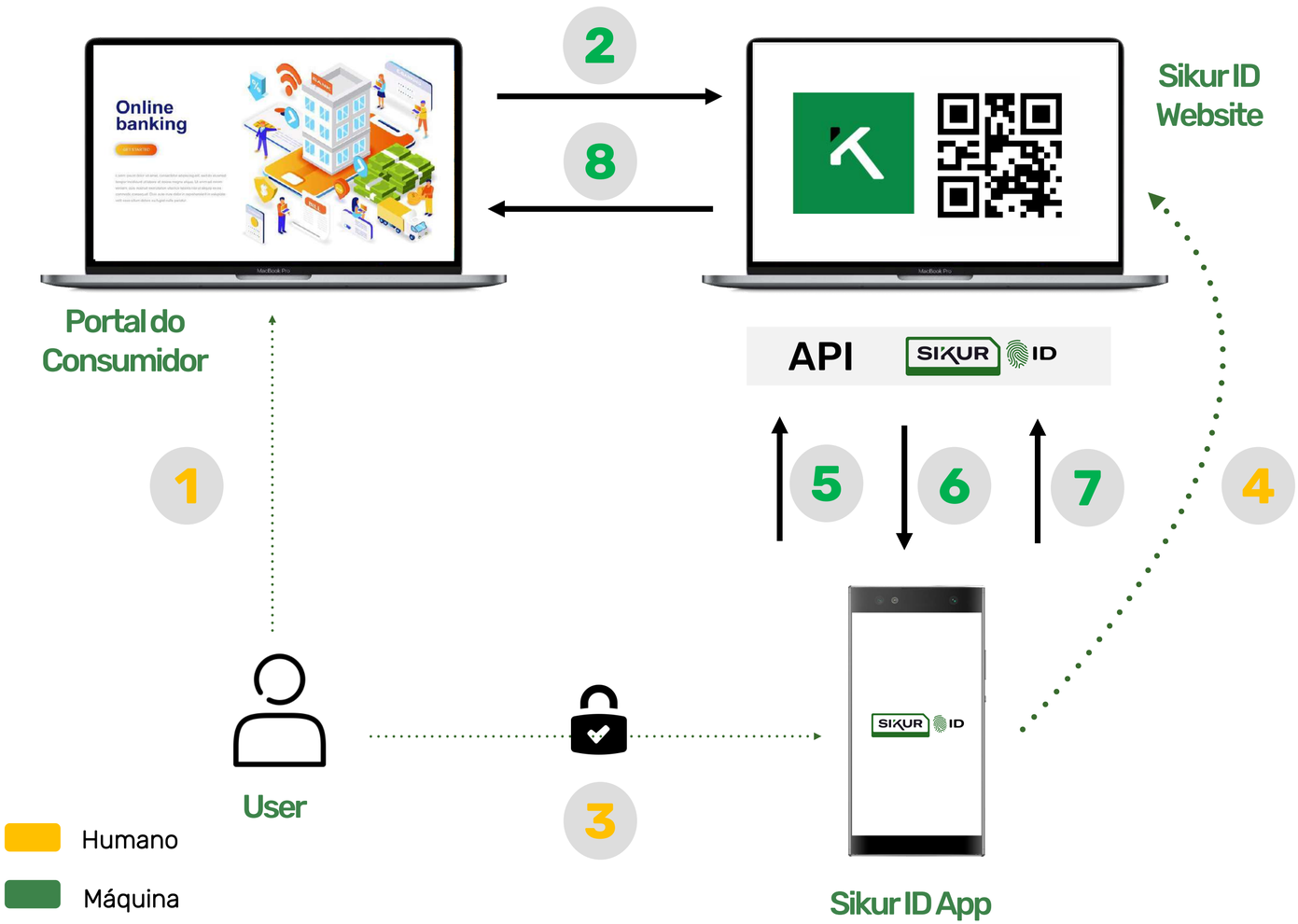
* Hardware Security Module

A Solução

Autenticação forte e proteção de chaves privadas para múltiplos cenários e aplicativos.



A Solução – passo a passo - site



1. Usuário acessa o portal do consumidor para autenticar
2. Portal liga para o site do Sikur ID e gera o QR Code
3. Usuário acessa o aplicativo Sikur ID com sua impressão digital
4. Usuário verifica QR Code através do Aplicativo
5. O aplicativo Sikur ID vai para a API Sikur ID e pede para associar o usuário ao QR Code. A API pede que o usuário prove que sua identidade, através de um desafio que é enviado para o aplicativo
6. O usuário, em posse da chave privada, resolve o desafio enviado pela API
7. APi associa o usuário ao QR Code
8. O usuário pode acessar o sistema

Cases

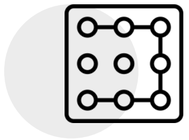
B2B2C
Banco Tradicional

B2B2C
Banco Digital

B2B
Sistema de Automação
Web (apenas)

B2B
Sistema de Automação
Web e App

O Produto - Resumidamente

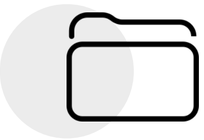


Segurança Digital

Uma plataforma de autenticação, adequada para os ambientes mais exigentes.
Em termos industriais, adaptáveis para diferentes tipos de sistemas

Provedor de Identidade

Faça login e inscreva-se
Gerencie a identidade sem esforço, com forte proteção para as chaves privadas do usuário



Diretório Inteligente

Conectar e autenticar sistemas novos e existentes
Controle de usuário e permissão dentro de Aplicativos e Sistemas

Auditoria e Conformidade

Monitoramento e alerta
Cumprir as normas

O Produto – Módulos

O Provedor de Identidade

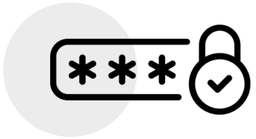
Um diretório de usuário seguro para a Organização, mais seguro do que nome de usuário e senha

Ele usa um processo de autenticação único, fazendo uso das chaves privadas do cliente

Algo único e que não pode ser transferido, como a biometria

Faça uso de protocolos padrão da indústria

Conecte a identidade digital à pessoa real usando a biometria, que é algo único



EM BREVE

Smart MFA

Melhorar os processos de autenticação existentes

Plugável, fácil de conectar com o seu sistema existente e fácil de atualizar

Offline: gera códigos autenticação sem conexão com a Internet

Leve-o com você e substitua-o facilmente, quando necessário

Faça uso de protocolos padrão da indústria

Conecte a identidade digital à pessoa real usando a biometria, que é algo único

EM BREVE

Data Key *

Criptografia de ponta a ponta usando chaves privadas

Mais segurança: adicione uma camada de segurança extra com criptografia

Selecione e criptografe partes de dados usando nossa API e sua chave privada

Não-repúdio no nível de dados do usuário

EM BREVE

Chain*

Não-repúdio no nível de transação

Proteger dados registrando cada transação, em um processo transparente e verificável

Cresça seguro com a rede Sikur Blockchain

*** Esses produtos dependem do Provedor de Identidade ou do Smart MFA**

Melhore, à medida que você implementa

Os principais ataques que protegemos

Os principais ataques

- Força bruta
- Roubo de token/chave privada
- Ataque homem-no-meio
- Replay de autenticação
- Auth spoofing
- **Phishing**

65%

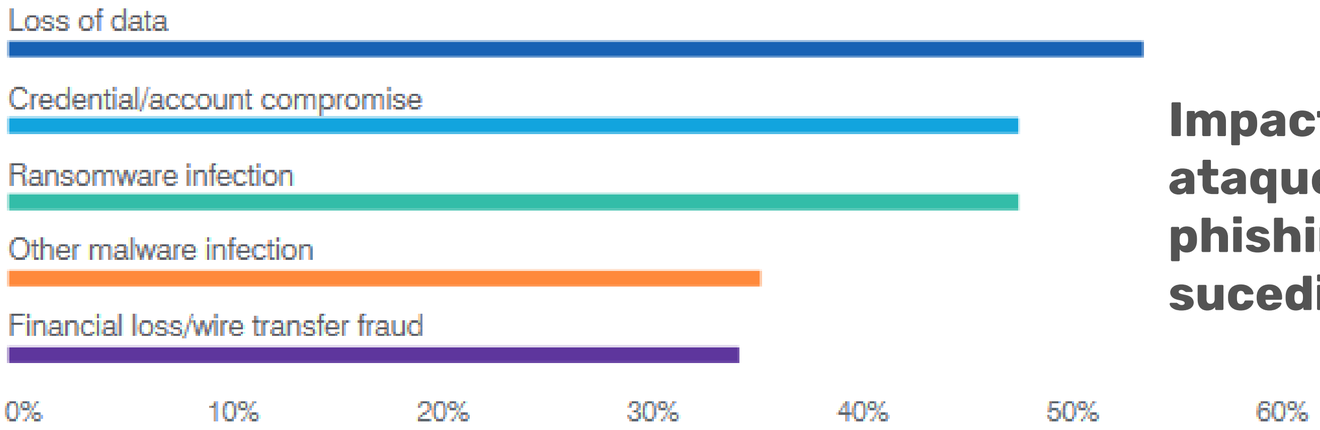
As organizações americanas sofreram um ataque de phishing bem sucedido no ano passado, bem acima da média global de 55%.

42%

As organizações japonesas sofreram um ataque de phishing bem-sucedido em 2019, a menor taxa de incidentes em todas as regiões pesquisadas.

60%

Of U.S. organizations experienced a successful credential phishing attacks, higher than the 47% global average.



Impactos de ataques de phishing bem sucedidos

Source: Proofpoint State of the Phish Report, 2020

Diferenciais de Produto

1. **Proteção de chave privada**
   apenas o usuário tem acesso a ele
2. **Não-repúdio**
   Compatível com blockchain, controle e conformidade
3. **Conformidade com o Regulamento de Proteção de Dados***
   proteção de dados com chaves de usuário, privadas
4. **MFA protegido**
   forte e flexível
5. **Proteção e criptografia de sistemas legados**
   com chaves privadas de usuário, suportadas pelo MFA
6. **Modelo de Negócio**
   nuvem ou no local e White Label
7. **MFA inteligente para resolver phishing**
   Senhas são o inimigo da segurança
   Tudo é suspeito, menos seu Sikur MFA.
   Hackers encontrarão uma maneira de contornar controles extravagantes de IA ou ML

* GDPR, LGDP, indústria e países regulação específica

Cases

1

Como provedor de identidade

Você pode usar o Autenticador Sikur para autenticar sistemas legados ou construir novos esquemas de autenticação.
Que tal ter um "Inscreva-se ou Faça Login com o Sikur" em sua página web ou Aplicativo?

2

Migrar e Integrar

Duvidando do seu provedor de autenticação existente? Migrar fácil para o Sikur ID. Quer manter seu esquema de autenticação e torná-lo mais forte? O Aplicativo Autenticador Sikur ajudará com isso.

3

Segundo Fator de Autenticação

O processo de autenticação, devidamente reforçado.
Um método robusto para bloquear phishing.

4

Quadro De Auth

Não quer construir um esquema de autenticação do zero? O Sikur ID pode fornecer credenciais para o seu Aplicativo e Sistemas

5

Transações, garantidas

Funciona como uma seguradora de transações, como o conceito Blockchain, entregando não-repúdio

Mercado-alvo e Suporte Estratégico

Defesa
Governo
Corporativa
Telco
Finanças
Varejo
Saúde

Internet das Coisas

Transações Digitais

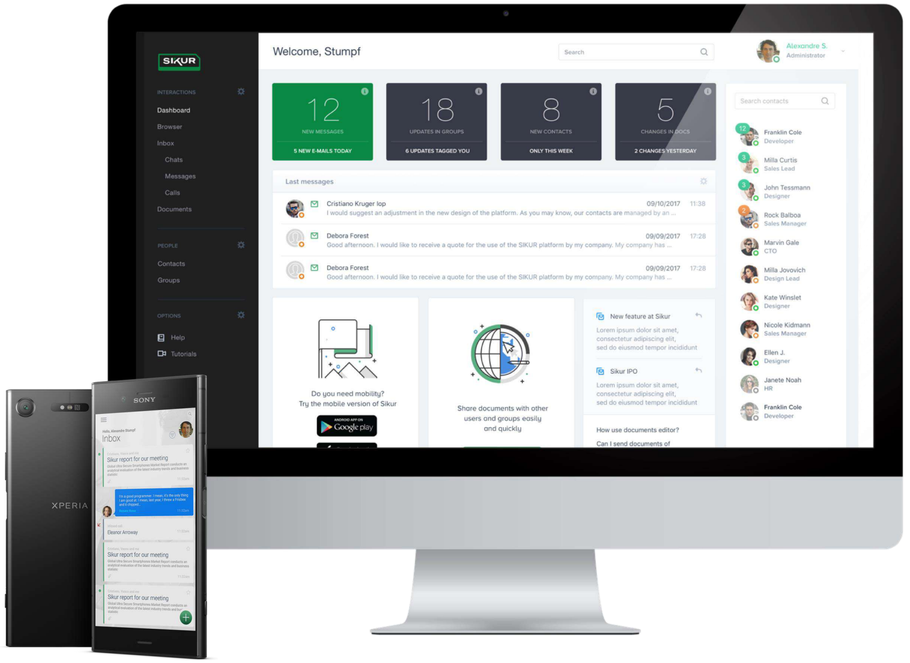
Aplicativos de terceiros

Regulamentar

Case

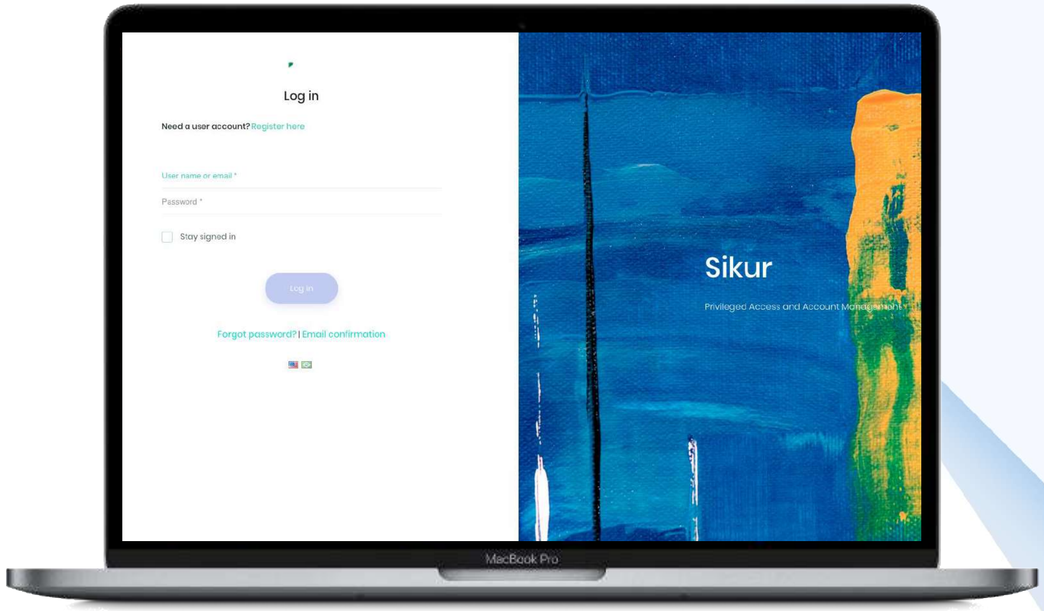
SIKUR Messenger - Global

- O esquema de autenticação mais maduro
- Comprovado em Programas de Recompensa de Bugs
- Suporte a uma ampla base de usuários



VaultOne - Global

- Autenticação e controle
- Segurança multicamadas



Apêndice

Os Módulos – características

Soluções de Mercado - comparativo

Os Módulos – Características

	The Identity Provider	Smart MFA (COMING SOON)	Data Key (COMING SOON)	Chain (COMING SOON)
• Autenticação em nuvem	✓	✓	✓	✓
• Autenticação no local	✓	✗	✓ *	✓ *
• Proteção em camadas contra ataques	✓	✓	✓	✓
• Único sinal	✓	✓	✓	✓
• Integração SIEM	✓	✓	✓	✓
• RBAC: Controle de acesso baseado em função	✓	✓	✓	✓
• Criptografia de ponta a ponta	NA	NA	✓	✓
• Criptografia na origem, com chaves privadas do usuário	NA	NA	✓	✓
• Proteção de sistemas legados com criptografia	NA	NA	✓	✓
• Não-repúdio	NA	NA	✓	✓
• Transações verificáveis de processo transparente	NA	NA	✓	✓
• Rede privada Blockchain	NA	NA	✗	✓

* Somente com o Provedor de Identidade

Comparando com outras soluções de autenticação 2FA

Soluções de Mercado – Comparativo

Main Problems	SMS Token	Email Token	Hardware Token	Software Token	Phone Call	SIKUR ID	Como resolver?
• Proteger contra terceiros	✗	✗	✓	✗	✗	✓	• MFA auth, chaves criptografadas
• Dispositivo perdido, esquecido e perdido	✗	✗	✗	✓	✗	✓	• App acesso por fingerprint
• App deToken comprometido sem o conhecimento do usuário	✗	✗	✗	✓	✗	✓	• App acesso por fingerprint
• SIM Swap	✗	✗	✓	✗	✗	✓	• MFA auth, App fingerprint
• Phishing Ataque	✗	✗	✓	✗	✗	✓	• MFA auth, App fingerprint
• Man-in-the-middle Ataque	✗	✗	✓	✗	✗	✓	• MFA auth, strong encryption
• Ataque de replay de autenticação	✗	✗	✓	✗	✗	✓	• MFA auth, strong encryption
• Auth spoofing Attack	✗	✗	✓	✗	✗	✓	• Criptografia forte, PKI
• Ataque de força bruta	✗	✗	✓	✗	✓	✓	• MFA auth, camadas de segurança

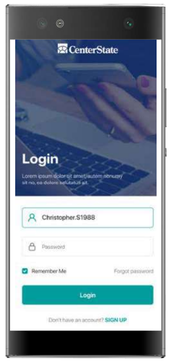
Retorno
Casos de uso

B2B2C Caso de uso – banco tradicional

1 O banco usa o Sikur ID SDK para sua solução de autenticação (primária ou alternativa)

2 O cliente vai até agência bancária para abertura de conta, cadastrar seu nome de usuário, senha e cadastrar sua biometria (se disponível no banco)

SDK SIKUR ID ⟷ **API do banco**



3 O cliente baixa o aplicativo do banco da Apple ou Google Stores e faz o primeiro login com nome de usuário e senha a partir de (2), e cria a chave pública e privada do usuário. No primeiro acesso, ativa a biometria (cenário ideal, que deve ser obrigatório para melhor segurança, caso o banco a exija). A partir do segundo acesso, o cliente pode acessar o App usando biometria ou nome de usuário e senha.

4 Ao acessar o site do banco, ele mostrará um QR Code digitalizado

5 O cliente abre o App móvel com sua biometria ou nome de usuário e senha, vai para a área de autenticação para que o App possa ler o QR Code, permitindo acesso ao site

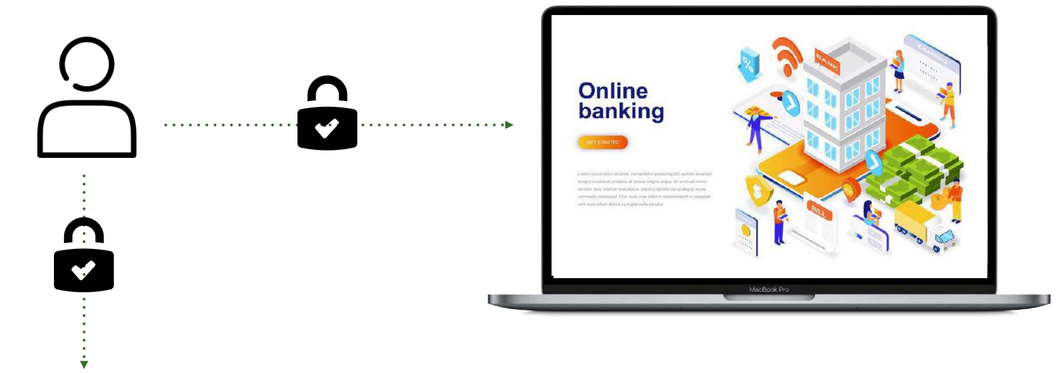
6 Dependendo dos processos bancários, as autorizações de transações podem utilizar o mesmo processo de segurança

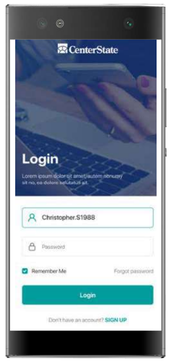
Retorno
Casos de uso

B2B2C Caso de uso – banco digital

1 O banco usa o Sikur ID SDK para sua solução de autenticação (primária ou alternativa)

SDK SIKUR ID ⋯⋯ **API do banco**





2 O cliente baixa o aplicativo do banco da Apple ou Google Stores e faz o primeiro login com nome de usuário e senha a partir de (2), e cria a chave pública e privada do usuário. No primeiro acesso, ativa a biometria (cenário ideal, que deve ser obrigatório para melhor segurança, caso o banco a exija). A partir do segundo acesso, o cliente pode acessar o App usando biometria ou nome de usuário e senha

3 Ao acessar o site do banco, ele mostrará um QR Code digitalizado

4 O cliente abre o App móvel com sua biometria ou nome de usuário e senha, vai para a área de autenticação para que o App possa ler o QR Code, permitindo acesso ao site

5 Dependendo dos processos bancários, as autorizações de transações podem utilizar o mesmo processo de segurança

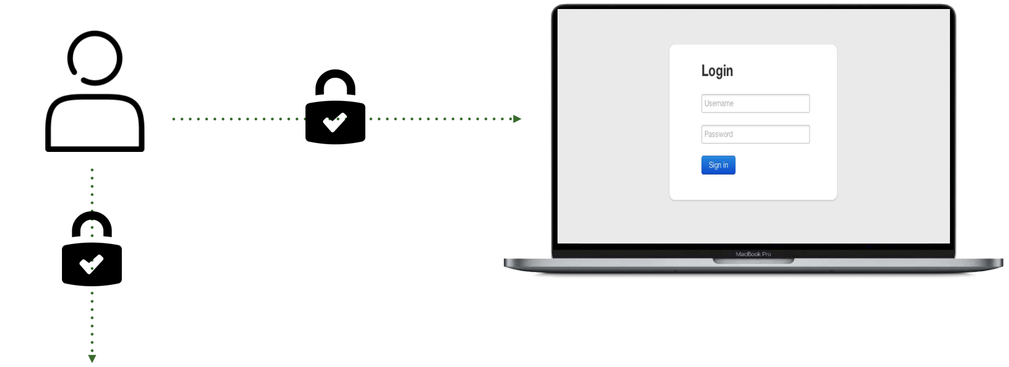
Retorno
Casos de uso

B2B Caso de uso – Sistema de Automação (somente Web)

1 O cliente usa o Sikur ID SDK para sua solução de autenticação (primária ou alternativa)

SDK SIKUR ID **API do sistema**

2 Todos os usuários criam contas de ID Sikur, registrando nome de usuário e senha



3 O cliente baixa o aplicativo de autenticação da Apple ou Google Stores e faz o primeiro login com nome de usuário e senha, criando a chave privada e pública. No primeiro acesso, após a entrada no PIN, a biometria está disponível para ativação. A partir do segundo acesso, o usuário pode acessar através de PIN ou biometria. Este aplicativo pode ser rotulado em branco

4 Ao acessar o site, ele mostrará um QR Code digitalizado

5 O cliente abre o Sikur ID com um PIN ou biometria, vai para a área de autenticação para que o App possa ler o QR Code, permitindo o acesso ao site

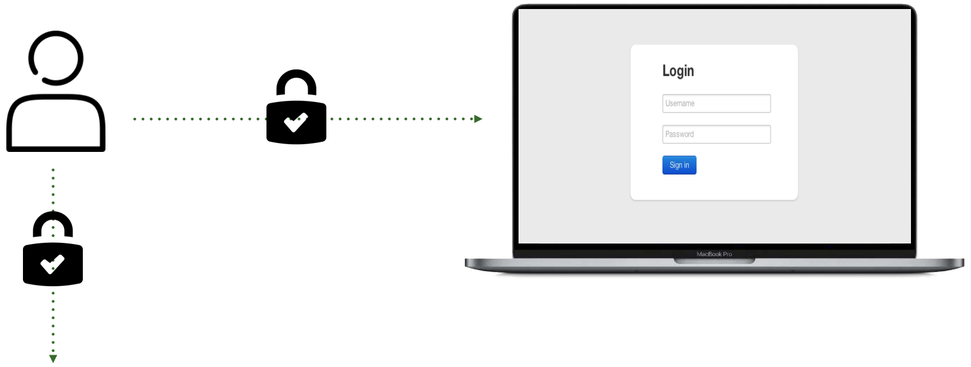
Retorno
Casos de uso

B2B Caso de uso – Sistema de Automação (Web e App)

1 O cliente usa o Sikur ID SDK para sua solução de autenticação (primária ou alternativa)

2 Users create their accounts in the automation system, enrolling username and password

SDK SIKUR ID ⟷ **API do sistema**



4 Ao acessar o site, ele mostrará um QR Code digitalizado

5 O cliente abre o sistema de automação com sua biometria ou nome de usuário e senha, vai para a área de autenticação para que o App possa ler o QR Code, permitindo acesso ao site

3 O cliente baixa o aplicativo de autenticação da Apple ou Google Store e faz o primeiro login com nome de usuário e senha, criando a chave privada e pública. No primeiro acesso, após a entrada no PIN, a biometria está disponível para ativação. A partir do segundo acesso, o usuário pode acessar através de PIN ou biometria.

We are the new secure communication mindset