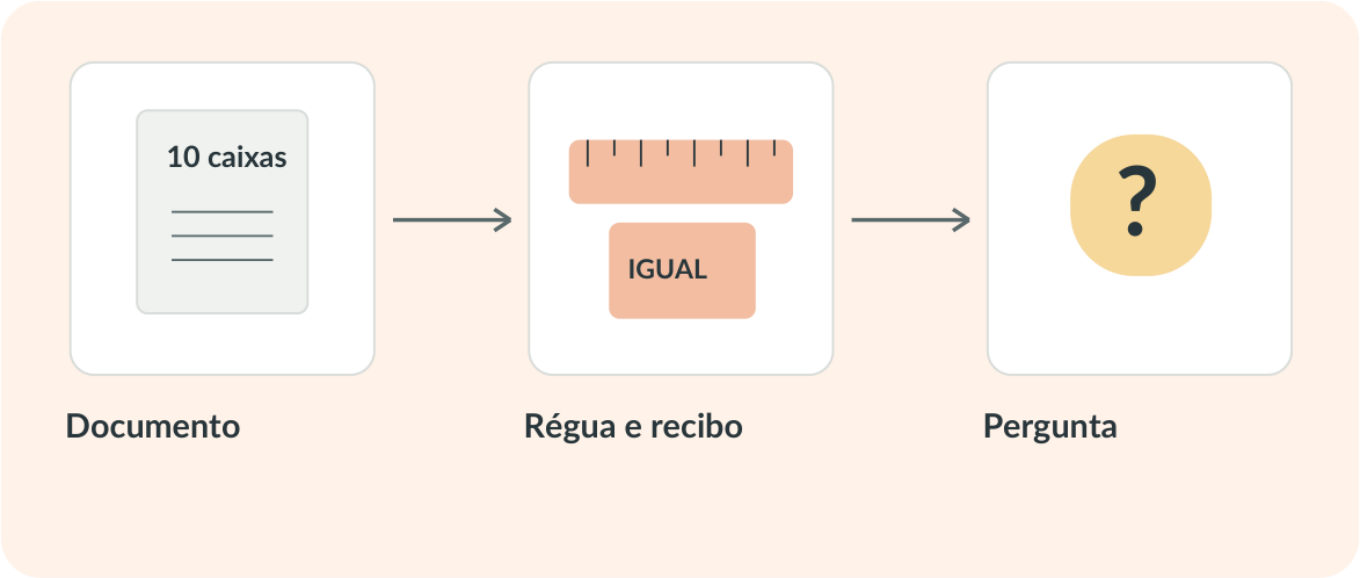
O PRINCÍPIO

O que sabemos, como conferir, o que ainda não sabemos

Um guia da Konfirmu para famílias, professores, decisores e profissionais.



Duas folhas dizem que chegaram dez caixas. Uma pessoa vai ao armazém, conta as caixas no chão e encontra nove.

Conseguimos confirmar que as folhas são iguais. Para saber quantas caixas chegaram, precisamos também da contagem. Que prova pedirias a quem as recebeu?

TRÊS DEGRAUS DA EVIDÊNCIA

O que se pode confirmar?

Uma cópia, uma assinatura e uma contagem respondem a perguntas diferentes.

01 Temos uma referência de confiança?

Pode ser o ficheiro original ou uma impressão digital do ficheiro, obtida por um canal de confiança. Guarda também a versão e a origem da referência.

02 A cópia mantém os mesmos dados?

Um hash é uma impressão digital calculada a partir dos bytes de um ficheiro. Uma assinatura digital, conferida com uma chave de confiança, permite ainda verificar a ligação à chave de quem assinou.

03 O que está escrito aconteceu?

Para esclarecer o facto, podes ter de contar as caixas, conferir uma medição, consultar um registo oficial ou pedir a revisão de uma pessoa com competência para o fazer.

Três respostas possíveis

«Igual» quando a comparação coincide. «Diferente» quando há uma divergência. «Ainda não sei» quando falta a referência ou outro elemento da prova.

É possível conferir sem internet se o aparelho já tiver os dados, a referência e as ferramentas. Um original perdido só pode ser recuperado se existir uma cópia.

DESCOBRIMOS / COMO CONFERIR / O QUE ISTO NÃO GARANTE

Os erros que aprendemos a ver

Seis resultados da nota científica de 25 de novembro. O estado de cada ensaio refere-se à versão identificada na nota.

DESCOBRIMOS	COMO CONFERIR	O QUE ISTO NÃO GARANTE

F1 Uma margem de 95% pode cobrir menos

Neste exemplo, a margem superior calculada pelo método linear cobre 86,51% dos valores, embora o nível nominal seja de 95%.	A página 7 mostra como calcular a cobertura para o inverso de uma variável normal de média 1 e desvio-padrão 0,3.	O resultado aplica-se ao modelo e aos limites indicados. A sua extensão a outras medições requer um novo cálculo.

F1 recalculado para esta edição. A equipa também repetiu o cálculo em 24 de novembro.

F2 O recibo e o tamanho do lote

Em certos lotes, o recibo da versão estudada deixou por confirmar a quantidade de elementos.	Uma revisão deve registar quantas peças foram recebidas e que evidência vincula essa contagem ao recibo.	O resultado limita o que se pode concluir sobre o lote. A nota não apresenta uma quebra do algoritmo SHA-256.

F2 repetido pela equipa em 24 de novembro. A nota registou o ponto como aberto na versão 3.0.0.

F3 Quando se perde uma distinção nos dados

A representação guardada perdeu uma distinção que existia nos dados de origem. O recibo deixou de a conseguir comprovar.	Na revisão, a equipa deve conseguir mostrar que todas as distinções relevantes no original se mantêm no registo.	A perda ocorreu na representação dos dados. Este ensaio não demonstra uma colisão criptográfica.

F3 repetido pela equipa em 24 de novembro. A nota registou o ponto como aberto na versão 3.0.0.

DESCOBRIMOS / COMO CONFERIR / O QUE ISTO NÃO GARANTE

Quando a máquina tem de parar

Seis resultados da nota científica de 25 de novembro. O estado de cada ensaio refere-se à versão identificada na nota.

DESCOBRIMOS	COMO CONFERIR	O QUE ISTO NÃO GARANTE

F4 Dois verificadores deram respostas diferentes

A revisão interna relata a deteção de 7 em 9 alterações num verificador e de 9 em 9 no outro.	Para avaliar uma nova versão, é preciso comparar as decisões com as esperadas e conservar os recibos dos ensaios.	Nove exemplos não permitem determinar quantas alterações seriam detetadas noutro conjunto de documentos.

F4 relatado na revisão interna de 24 de novembro. A equipa não repetiu o ensaio para a nota.

F5 Um «OK» onde a regra exigia paragem

A equipa identificou quatro situações em que a resposta foi «OK», embora a regra determinasse «VETO».	Com a correção proposta, 186 dos 1 246 casos deixaram de dar «OK». Nenhum passou a dar «OK».	A nota descrevia uma proposta de correção. A aplicação em produção exige prova da versão instalada e dos testes.

F5 relatado em 24 de novembro. A nota de dia 25 indicava que a correção ainda não era pública.

F6 Uma leitura muito perto do limite

Num exemplo com limites de 2 a 8, a leitura arredondada a seis casas decimais e a leitura de maior precisão levaram a decisões diferentes.	A revisão deve identificar a precisão usada e a regra acordada para comparar a medição com o limite.	A tolerância depende da finalidade e da regra aplicável. O resultado deste exemplo não fixa tolerâncias para outros usos.

F6 relatado em 24 de novembro. À data da nota, a regra de referência continuava em discussão.

SAÚDE E MEDICINA

Conferir um registo de saúde

Três situações fictícias em que uma pessoa pode comparar um registo com uma referência de confiança.

01 Um registo de vacinação

A comparação pode revelar que uma cópia foi alterada. Para saber se a vacina foi administrada são precisos elementos do ato clínico. A eficácia exige evidência própria.

02 O resultado de uma análise

É possível conferir se o relatório recebido corresponde ao guardado pelo laboratório. A interpretação de um resultado real cabe aos profissionais de saúde.

03 Um registo de cadeia de frio

É possível conferir se a cópia do histórico coincide com a referência. A calibração do sensor e as condições reais de conservação precisam das suas próprias verificações.

Um sensor pode registar um valor errado

Suponhamos que um sensor regista 4 °C. Se estiver avariado, a temperatura real pode ser outra, mesmo que a cópia do registo coincida com o original.

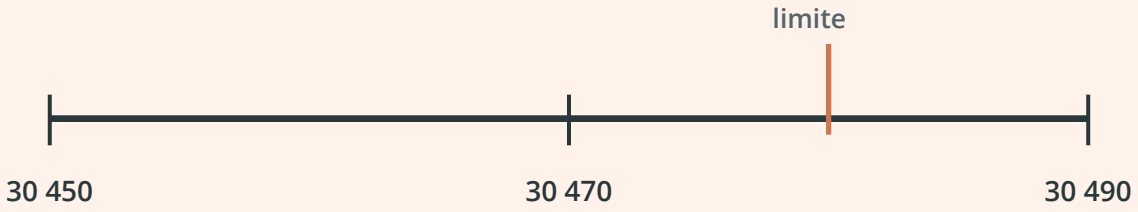
A Konfirmu é descrita na nota científica como um protótipo de investigação. Não é um dispositivo médico e não foi concebida para diagnóstico, tratamento ou decisões sobre pessoas.

SEGURANÇA OPERACIONAL E VOTO

Um recibo válido pode dizer «pare»

Ensaio de bancada com um contentor fictício e um limite hipotético de 30 480 kg.

Pesagem de 30 470 ± 20 kg



Intervalo da pesagem, em quilogramas

O intervalo vai de 30 450 a 30 490 kg. A folga, calculada como limite menos peso, vai de −10 a +30 kg. No extremo superior, o peso excede o limite em 10 kg. O recibo pode ter uma assinatura válida (VALID) e a regra indicar paragem (VETO).

E numa votação?

Conferir uma ata assinada permite detetar alterações posteriores. O acesso dos eleitores, a exatidão da contagem e o segredo do voto exigem provas próprias. Um recibo que revele a escolha de uma pessoa pode comprometer esse segredo.

Quem pode autorizar a operação?

A assinatura permite verificar o documento. A decisão real de avançar cabe às pessoas responsáveis, com as normas e os dados próprios da operação.

VERIFICAÇÃO NO PRÓPRIO APARELHO

Como conferir por ti próprio

Com uma referência de confiança, podes comparar um ficheiro. Também podes repetir a conta estatística da página 3.

Na nota, a versão de referência do motor é a 3.0.0, identificada pelo commit 90b3968, de 24 de novembro de 2026. A licença do código é EUPL-1.2.

Repositório oficial do código

github.com/silvadvp-del/konfirmu-claim-protocol

SHA-256 do motor, conforme declarado na nota

`529098c652ee8234960d69383e308f60db6a5df8ea6bdae578b538eb806e80cf`

Se tiveres o manifesto SHA256SUMS.txt da versão e os ficheiros correspondentes na mesma pasta, podes compará-los com um dos comandos seguintes.

```
sha256sum -c SHA256SUMS.txt       # Linux
shasum -a 256 -c SHA256SUMS.txt   # macOS
```

A equipa relatou 62 ficheiros conformes, 247 autoverificações e 10 conjuntos de regras testados em Linux com Python 3.13. São números dessa revisão.

F1 · Uma conta que podes repetir em Python

```
from statistics import NormalDist
X, Z = NormalDist(1, 0.3), NormalDist()
u = 1 + Z.inv_cdf(0.95) * 0.3
print(u, X.cdf(0) + 1 - X.cdf(1/u))
print(X.cdf(1/0.412) - X.cdf(1/1.588))
```

Para Y = 1/X, o limite superior é 1,493456088 e a cobertura é 86,51%. A conta inclui os valores de X abaixo de zero, que também satisfazem o limite. Com os limites bilaterais arredondados publicados, de 0,412 a 1,588, a cobertura é 89,14%.

A cobertura é a probabilidade prevista por este modelo. Os documentos JCGM 100 e 101, citados na nota, enquadram a propagação da incerteza.

LIMITES E PRÓXIMOS TESTES

O que ainda não sabemos

Uma prova pode ser conferida por quem a recebe. O alcance dessa prova depende da referência e do teste realizado.

Quem fez os testes?

A nota de 25 de novembro atribui os testes à equipa e a sistemas de IA ao seu serviço. Para uma revisão independente, outra equipa terá de identificar a versão, repetir os ensaios e registar os resultados, incluindo as divergências.

Que reconhecimento existe?

A análise dos 295 requisitos da ECSS-Q-ST-80C Rev.2 foi uma autoavaliação. Os depósitos i-DEPOT 162925 e 164391 documentam o conteúdo depositado e as respetivas datas. A qualidade do produto exige avaliação própria.

O que se pode concluir de um carimbo de tempo?

O Chronolex permite conferir a integridade dos registos. A nota assinala que o serviço público gratuito de carimbos de tempo usado não oferece valor legal garantido. A ocorrência do acontecimento requer evidência adicional.

Encontraste uma divergência?

Guarda a versão, o resultado esperado e o resultado observado. Envia a descrição à equipa através de admin@dpsindustrial.nl.

Fonte primária · Nota científica de 25 de novembro de 2026

Konfirmu_Scientific_Note.pdf · 88 212 bytes · SHA-256

`884fde70000fa68dccdb4b6527da7a1bce8a7737b3f44c03340f182ae6100f88`

DPS Industrial & Maritime Services · Konfirmu

Enschede, Países Baixos · KVK n.º 42005886 · admin@dpsindustrial.nl