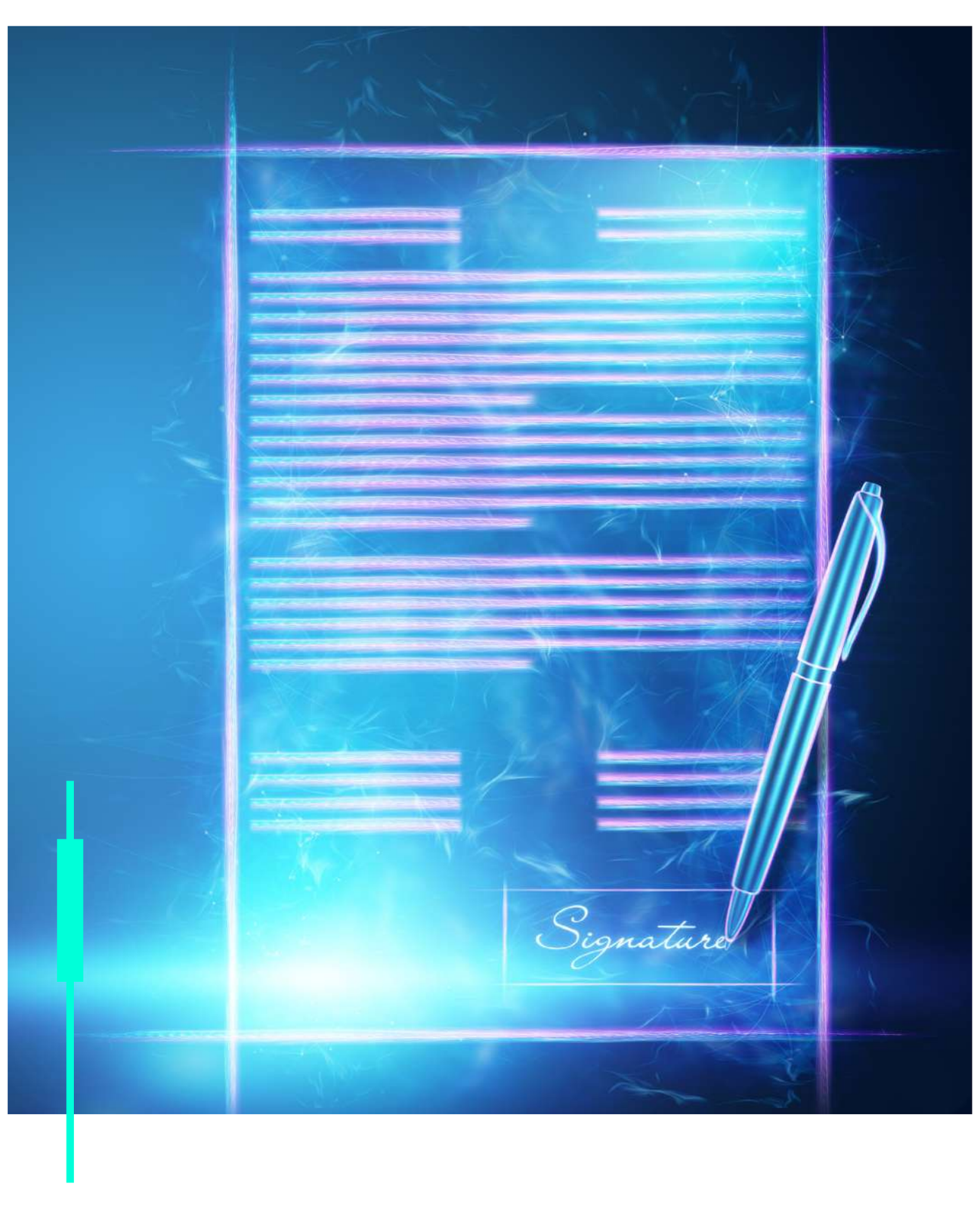
KRYPTUS shaping trusted bonds | ITI Instituto Nacional de Tecnologia da Informação

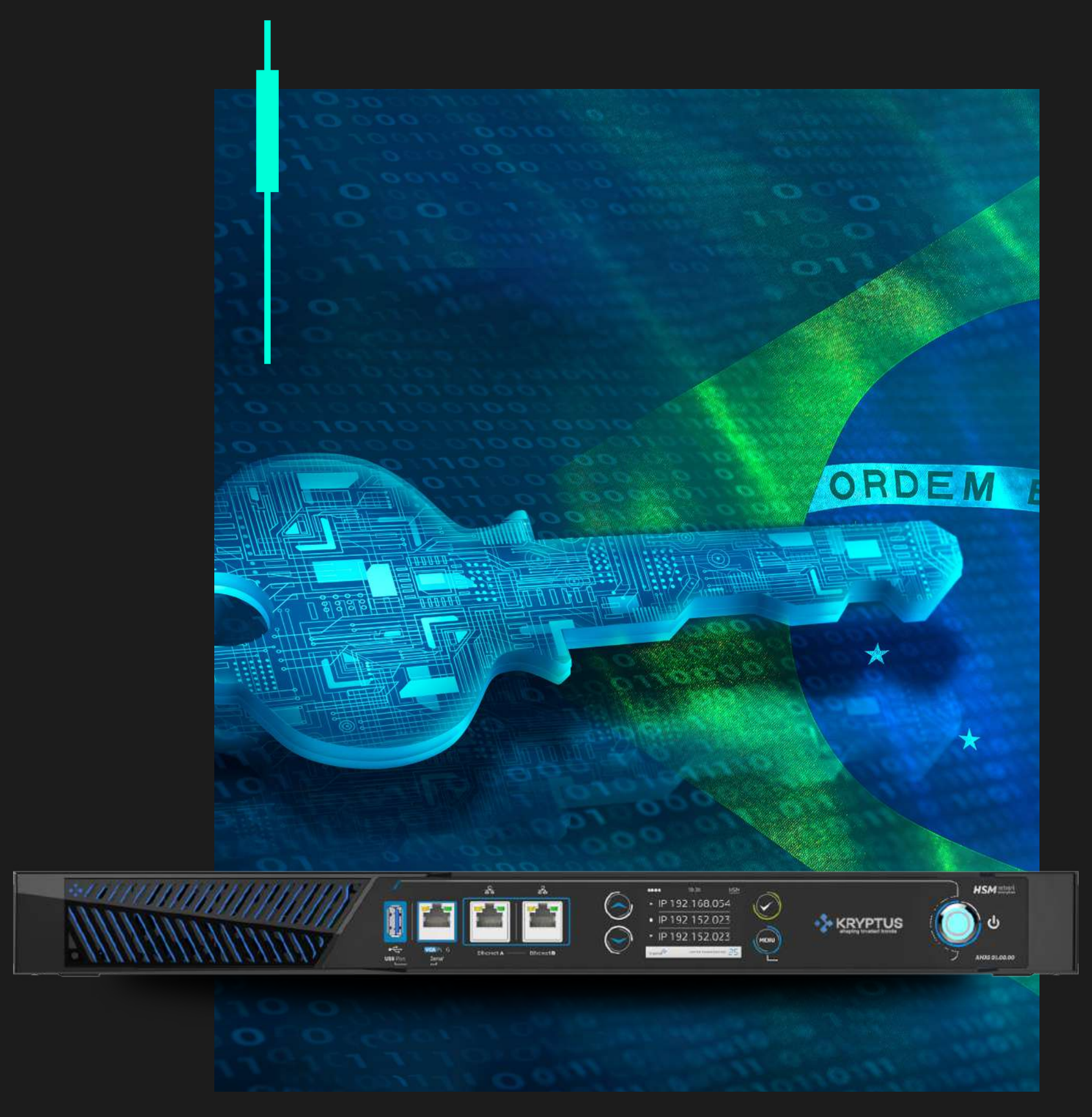
ITI E KRYPTUS: PARCERIA ARROJADA NA INOVAÇÃO DA ICP-BRASIL

Responsável pelo padrão público de certificação digital no país, a Infraestrutura de Chaves Públicas Brasileira - ICP-Brasil, tendo à frente o Instituto Nacional de Tecnologia da Informação – ITI, completa 20 anos de um projeto inovador. Nessa trajetória de duas décadas, a Kryptus, multinacional brasileira provedora de soluções de criptografia e segurança cibernética, foi parceira em importantes conquistas. Para recapitular essa história de sucesso, Roberto Gallo, CEO da Kryptus, entrevistou Maurício Coelho, diretor de ICP do ITI.



MODELO DE ICP PÚBLICO-PRIVADA.

Originalmente projetada para operar exclusivamente no âmbito governamental, a ICP-Brasil logo abriu-se para um modelo público-privado. "Ali, em 2001, já houve um primeiro momento de inovação ao se propor uma infraestrutura aberta à sociedade, com um modelo de característica híbrida", lembra Coelho. "Temos participação de entidades públicas e, majoritariamente, privadas, que respondem por 90% das emissões da ICP-Brasil. Hoje temos mais de 2 mil entidades credenciadas, é um modelo que se mostrou acertado", comemora o diretor do ITI.



LADO A LADO NA GERAÇÃO DE TECNOLOGIA NACIONAL PARA GESTÃO DE CERTIFICADOS.

O início das operações foi no Serpro, à época no Horto, no Rio de Janeiro. Naquela ocasião, recorda Coelho, o ITI não tinha um ambiente próprio e contava com solução criptográfica, de sistema gerenciador e HSMs de um provedor fechado estrangeiro, que oferecia pouca flexibilidade. "Ali tivemos o primeiro grande desafio, de como sair daquela condição de refém de uma solução".

Foi então, em 2003, que o primeiro grande projeto de inovação para o ICP-Brasil veio à tona, com o objetivo de desenvolver um sistema gerenciador de certificados nacional com tecnologia própria. Sob coordenação do ITI, o projeto - batizado João-de-Barro - contou com vários parceiros, como o LabSEC (UFSC), CASNAV (Marinha), RNP e Kryptus, que participou do desenvolvimento do hardware responsável pela implantação, em 2008, do sistema gerenciador de certificados IUAPA - denominação índigena para "raiz" -, já em ambiente próprio do instituto, localizado em Brasília.

"Em 2001 foi emitida a raiz v0, a primeira raiz. Com o HSM provido pela Kryptus", prossegue Maurício Coelho, "em 2008 emitimos a raiz v1, essa já em solução nacional, a primeira raiz em solução 100% brasileira de hardware e software. Foi um passo de inovação muito interessante, e desde aquele momento tivemos a contribuição de vários parceiros, e destaco aqui a contribuição da Kryptus".

INTEROPERABILIDADE GARANTIDA ENTRE EQUIPAMENTOS CRIPTOGRÁFICOS.

Outro ponto destacado pelo diretor do ITI diz respeito ao processo de homologação de equipamentos criptográficos no Brasil. "Tínhamos, desde sempre, as homologações internacionais, porém sentimos a necessidade de alcançar não só as questões técnicas, criptográficas, mas também as questões de interoperabilidade", pontua. "Por exemplo, quando um usuário tinha um cartão inteligente da empresa A e precisava utilizá-lo na leitora da empresa B, não interoperava e vice-versa, ou quando a gente precisava fazer a troca de HSMs e não funcionava. Então, novamente tivemos a contribuição de vários parceiros da indústria que envolve esses dispositivos (cartões, tokens, HSMs), e a Kryptus, conosco mais uma vez, para idealizar esse sistema de homologação, que nasceu como uma homologação interna no ITI. Conduzíamos todo o processo e tinha a parceria do LSI-TEC, da USP, como laboratório de ensaios, e o HSM da Kryptus foi o primeiro a ser homologado pela ICP-Brasil, justamente por ser o HSM que a gente aplicou na AC Raiz, em 2008, nessa solução que veio da v1".

ALGORITMOS MAIS SEGUROS À FRENTE DAS AMEAÇAS.

Em 2010 foi emitida a raiz v2, com segurança criptográfica mais robusta; e, no mesmo ano, a raiz v3 - primeira a contar com curvas elípticas. Coelho aponta, no entanto, que os vazamentos do caso Snowden, em 2013, trouxeram um novo desafio. "Houve uma suspeição dessas curvas, da possibilidade de haver alguma questão de backdoor, e como no âmbito da ICP-Brasil sempre priorizamos a segurança total, o comitê gestor decidiu revogar a raiz v3 em 2014".

Um ano depois, em um processo que novamente contou com o apoio da Kryptus e de outros setores da indústria e da academia, foi emitida a raiz v4, com curvas elípticas brainpoolP512. "Essa raiz foi adotada pelo Ministério das Relações Exteriores para a assinatura de passaporte eletrônico brasileiro, elevando-o a um padrão de segurança fantástico, é mais um case importante para o país", orgulha-se Coelho.

No final de 2018, foram adotadas as curvas Edwards, com a emissão de duas raízes: v6 (edwards448) e v7 (edwards521) - essa última, explica Coelho, "uma curva já padronizada por pesquisadores brasileiros, a única raiz no mundo, até onde se tem conhecimento, de PKI a adotar essa curva, considerada uma das mais seguras". Ele prossegue: "Esse trabalho em cima da Edwards trouxe uma inovação muito interessante, que surgiu das discussões sobre a segurança das urnas criptográficas brasileiras, e foi justamente a partir desse trabalho que surgiram as especificações, na verdade, todo o desenvolvimento de uma biblioteca criptográfica e da adequação do HSM da Kryptus, com a edwards521 sendo aplicada na confecção das novas urnas eletrônicas, que serão utilizadas no pleito de 2022".

REDUÇÃO DE CUSTOS PARA APLICAÇÃO DE CARIMBO DO TEMPO.

A mais recente parceria do ITI com a Kryptus envolve o desenvolvimento de um protocolo aberto de sincronismo e auditoria de tempo, já adotado pela ICP-Brasil neste semestre e, a partir do ano que vem, pelas autoridades de tempo credenciadas. "Vínhamos operando o sistema da entidade de auditoria do tempo, a EAT, que é a raiz do tempo brasileira, também operada pelo ITI, com uma tecnologia fechada. Com a adoção desse protocolo aberto, outras indústrias também poderão desenvolver equipamentos - sincronizadores ou carimbadoras -, ampliando, assim, a oferta e reduzindo os custos. Afinal, o carimbo de tempo é um insumo importantíssimo nas assinaturas eletrônicas, trazendo a evidência temporal da realização daquela assinatura. Não poderia deixar de destacar essa inovação, a mais recente em que estamos trabalhando", conclui Coelho.

SOBRE A KRYPTUS.

A Kryptus é uma multinacional brasileira provedora de soluções de criptografia e segurança cibernética altamente customizáveis, confiáveis e seguras para aplicações críticas, com foco na entrega de serviços de alto nível para resolução das missões de seus clientes. Fundada em Campinas (SP), em 2003, atua hoje nos setores público e privado dos mercados do Brasil, LATAM, Europa, Oriente Médio e África, sendo reconhecida pelo Ministério da Defesa do Brasil com o selo EED – Empresa Estratégica de Defesa, além de contar com selo Gartner Cool Vendor.

A Kryptus oferece proteção qualificada para certificação digital corporativa e de Estado com suas soluções de Infraestrutura de Chaves Públicas (ICP). Para porte nacional, a Kryptus realiza projetos de implantação de infraestrutura para instituições governamentais envolvendo a AC Raiz e todo o ecossistema de autoridades certificadoras. Para instituições interessadas em reduzir custos ao utilizar grande volume de certificados digitais, a Kryptus oferece uma solução completa para implantar uma AC Interna em ambiente corporativo. Fechando a gama de serviços da Kryptus para esse segmento, as AC's também podem contar com o apoio na implementação de uma AC de Tempo, onde o carimbo do tempo, associado a uma assinatura digital, estabelece evidência do instante de tempo em que documentos são assinados, gerados ou copiados em sincronia com uma fonte confiável de tempo e auditável por entidades certificadoras da ICP.

SAIBA MAIS

KRYPTUS shaping trusted bonds

HQ
+55 (19) **3112-5000**
fale.conosco@kryptus.com
www.kryptus.com
Rua Maria Teresa Dias da Silva 270
Campinas – SP, Brazil

EMEA
+41 **79 932 19 23**
kryptus.emea@kryptus.com
emea.kryptus.com
Rue Galilée 7, 1400, Yverdon
Switzerland

6421V2