PRESIDÊNCIA DA REPÚBLICA – CASA CIVIL
SCN – Quadra 2 Bloco E - 70712-905 – Brasília/DF
Telefone: (61) 3424-3853 / 3926/ 3875 – iti.gabinete@iti.gov.br

Projeto Certificação Digital em Nuvem (HSM/PSC da ICP-Brasil)

Briefing

1. Projeto – resumo

O Projeto de **Certificação Digital em Nuvem (HSM/PSC da ICP-Brasil)** visa, assim como feito no padrão europeu, entregar à sociedade brasileira uma nova forma para armazenar os certificados digitais dos usuários finais e regulamentar os portais de assinaturas digitais para dados, documentos e transações eletrônicas. Criar-se-á um novo ente na ICP-Brasil chamado de Prestador de Serviço de Confiança – PSC (semelhante ao TSP – Trust Service Provider na Europa), que será credenciado, auditado e fiscalizado pelo ITI, respeitando as normas que serão debatidas na COTEC e Consulta Pública, e, posteriormente, no Comitê Gestor da ICP-Brasil.

O PSC terá a tarefa primária de armazenar os certificados digitais dos usuários finais na ICP-Brasil, mantendo o controle, uso e conhecimento exclusivo por parte do seu titular, dentro de dispositivos criptográficos (HSM) que poderão estar em uma solução de nuvem, com alta capacidade de performance e segurança. Segurança, aliás, incrementadas aos normativos americanos e europeus, que garantirão, no mínimo, os mesmos requisitos dos dispositivos tipo smart card ou token em relação à proteção da chave privada do usuário final. A proposta é que, também, toda parte de autenticação do usuário fique dentro da fronteira física criptográfica do HSM e que as chaves dos usuários, mantendo o altíssimo nível de segurança, se utilize de um protocolo interoperável (KMIP – Key Management Interoperability Protocol); protocolo este que será testado junto com as Universidades parceiras do ITI, como a UFSC e UnB.

A segunda tarefa do PSC será padronizar todo o portfólio de assinaturas digitais no Brasil. A proposta é que se ofereça, caso assim o usuário deseje, um serviço de assinatura digital padronizado e de armazenamento dos documentos eletrônicos com toda proteção (que também será auditado e fiscalizado pelo ITI) e regulamentado pelo Comitê Gestor da ICP-Brasil, garantindo temporalidade (uso de sincronismo de tempo e carimbos de tempo da ICP-Brasil) e possibilidade de verificação por qualquer sistema ou software de verificação de assinaturas digitais. Pretende-se, então, que o usuário tenha sua vida facilitada quanto ao uso do certificado digital, sem se preocupar com atualizações de softwares ou programas, instalação de drivers, entre outros, assim como, que esse possa acessar o seu certificado digital por meio de qualquer dispositivo (celular, tablets, PC, entre outros), não havendo a necessidade de carregar um dispositivo para realizar as assinaturas digitais. Com isso, espera-se que haja uma redução de custo na ICP-Brasil e que essa torne-se mais amigável aos seus usuários.

2. Cronograma – estimativa

a) Estudos, reuniões técnicas e proposta de texto por parte do ITI (maio a setembro/2017) – Finalizado;

b) Reunião da COTEC – apresentação da proposta do ITI (15/09/2017);
Obs: Os membros da COTEC terão um mês para apresentar novas propostas.

c) Abertura para consulta pública e recebimento de propostas da sociedade (14 a 29/09/2017);

d) Testes de interoperabilidade e segurança dos HSM (03/10/2017 a 12/10/2017);
Obs: Parceria junto às Universidades para condução dos testes com o protocolo KMIP.

e) Apresentação das propostas da COTEC, da consulta pública e dos testes de interoperabilidade (15/10/2017 a 20/10/2017);

f) Redação final do texto deliberativo e entrega aos membros do Comitê Gestor da ICP-Brasil (20/10/2017 a 30/10/2017);

g) Reunião do Comitê Gestor da ICP-Brasil (10/11/2017).