

Revogação de Certificados na Infra-estrutura de Chaves Públicas Brasileira: Estado Atual e Alternativas

Marcelo F. Lima¹, Luiz Gustavo C. Silva¹

¹Departamento de Ciências Contábeis - Universidade Federal de Pernambuco (UFPE)
Recife, PE - Brasil
marcelo.lima.br@gmail.com, luiz.silva@ensinar.org

Abstract: *The Brazilian Public Key Infrastructure (PKI-Brazil) uses basic Certificate Revoked List (CRL), but in a brief future, with the sped up growth of the use of digital certificates in the national scope, the use of a more efficient model must be considered. On the basis of a survey and researches, the growth of the lists is evidenced. The results of the survey are applied in well known models of verification mechanisms and the impacts of the adoption of each model are evaluated. Considering performance and impact on the current model, the model that showed better results was the Over-Issued Segmented CRLs.*

Resumo: *A Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) usa Lista de Certificados Revogados (LCR) básica, mas em um futuro breve, com o acelerado crescimento do uso de certificados digitais no âmbito nacional, o uso de um modelo mais eficiente deve ser considerado. Com base em um levantamento e pesquisas, o crescimento das listas é evidenciado. Os resultados do levantamento são aplicados em modelos bem conhecidos de mecanismos de verificação e os impactos da adoção de cada modelo são avaliados. Considerando o desempenho e o impacto no modelo atual, o modelo que mostrou melhores resultados foi o Over-Issued Segmented CRLs.*

1. Introdução

A Infra-estrutura de Chaves Públicas Brasileira (ICP-Brasil) foi criada por força de lei [1] e é composta por diversas Autoridades Certificadoras (ACs). Baseia-se no modelo hierárquico [2, 3] e tem escopo nacional. Uma das funções das ACs é publicar Listas de Certificados Revogados (LCRs). Este trabalho demonstra o estado da verificação de revogação sob a ICP-Brasil, com base em dados reais levantados dos repositórios das ACs, e avalia mecanismos de verificação de revogação como alternativas para melhorar o desempenho desses serviços na ICP-Brasil. São levadas em consideração as ACs existentes em novembro de 2004.

Os certificados da ICP-Brasil, do certificado raiz [4] até as extremidades das cadeias, adotam o mesmo padrão [3]. Na prática isto quer dizer que todos os certificados têm as mesmas características básicas, mas podem conter variações que não comprometam as definições básicas.

A utilização de certificação digital no Brasil está em expansão. A 7ª Pesquisa Nacional de Segurança da Informação [5] de 2001 mostra que no item Principais Aplicações para Internet 1% dos pesquisados utilizavam certificação digital. Na 8ª [6]

pesquisa o percentual passa para 10%. Na 9ª [7] pesquisa o percentual chega a 24% e ela aponta que 50% dos pesquisados pretendiam adotar a certificação digital como medida de segurança.

2. Estado atual da revogação na ICP-Brasil

Não é exigido [1] na ICP-Brasil que um mecanismo diferente da LCR básica completa seja utilizado. Portanto, as ACs adotam as LCRs básicas. A frequência de emissão das LCRs varia para cada AC, podendo ser de uma hora ou de 24 horas.

Na ICP-Brasil as ACs emitem LCRs X.509 na versão 2 [8]. Quanto ao tamanho base da LCR e os bytes adicionais por entrada, a avaliação da ICP-Brasil condiz com os valores esperados [9] em uma infra-estrutura baseada no padrão X.509. A AC CertiSign SRF, por exemplo, tem uma CRL base com 494 bytes e mais 49 bytes adicionais por entrada de revogação. O levantamento demonstrou claramente que a AC com maior taxa de crescimento em sua LCR foi a AC CertiSign SRF. Do início ao final do período de levantamento a LCR da AC CertiSign SRF acumulou um crescimento de 201,96%, seguida pela AC SERASA CD (a partir de 23/04/2004), com 61,42%. O Gráfico 1 mostra o comportamento de todas as LCRs em relação ao percentual acumulado:

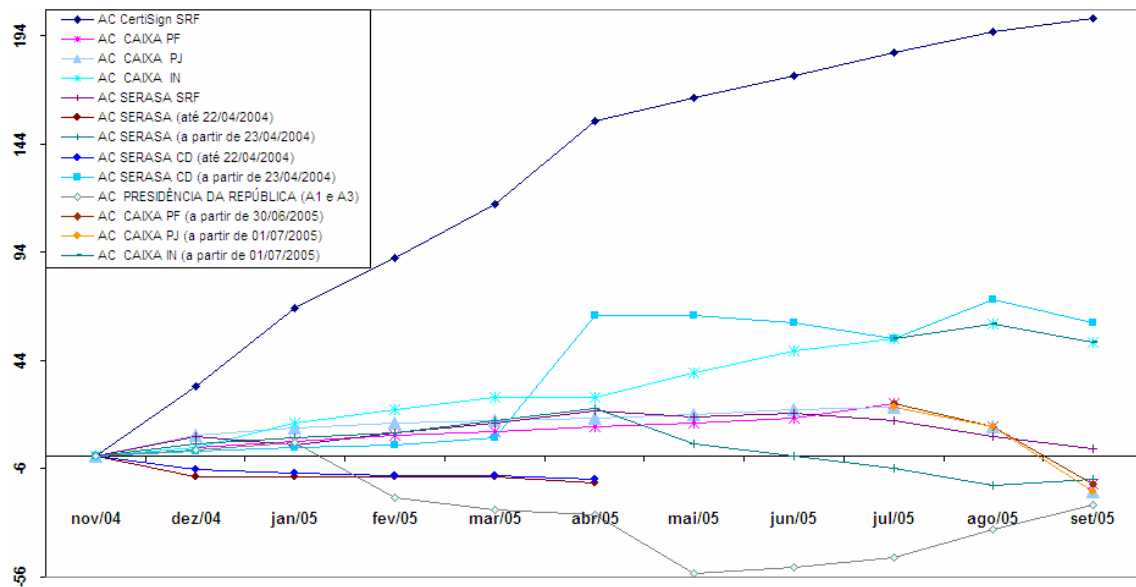


Gráfico 1. Percentual acumulado das LCRs da ICP-Brasil (nov/2004 até set/2005)

Além de apresentar o maior percentual acumulado de crescimento, a LCR da AC CertiSign SRF também se manteve com o maior tamanho absoluto durante praticamente todo o período de levantamento. LCRs maiores são mais custosas para serem obtidas. Se a LCR também for muito consultada, então haverá um maior esforço do repositório, pois ele terá que suportar mais carga nos momentos de picos de requisição. Os picos das taxas de requisição para uma LCR básica ocorrerão com a mesma frequência que a LCR é emitida. O pico ocorre no momento que a nova LCR torna-se disponível e a última LCR baixada, guardada no cache do verificador, expira.

O seguinte modelo descreve a taxa de requisição de um repositório em um tempo t [10]: $R(t) = Nve^{-vt}$. Definindo um cenário, o qual chamaremos de cenário ICP-Br, com 20.000 partes confiantes verificando uma média de 10 certificados por hora,

teríamos um pico de taxa de requisição no tempo 0 igual a 55,5556 req/s, como demonstrado no Gráfico 2.

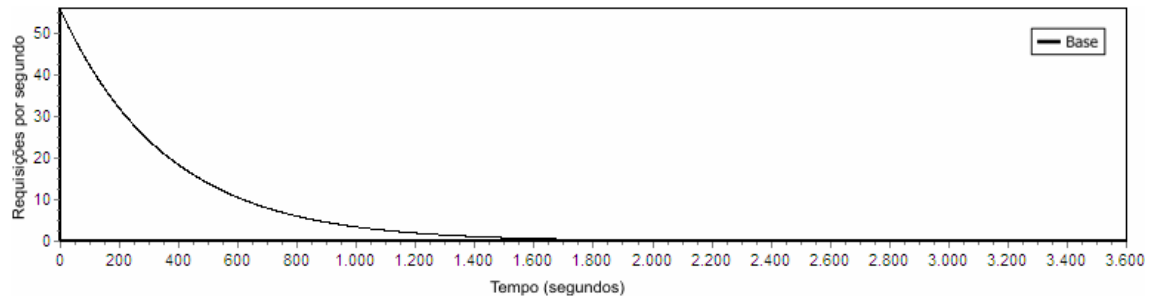


Gráfico 2. Taxa de requisição para CRL básica completa

A última LCR levantada emitida pela AC CertiSign SRF, que possui exatos 42.879 bytes, em um momento de pico de taxa de requisições resultaria em $42.879 \times 55,5556 = 2.326,3365$ Kbytes/s de consumo de banda.

3. Experimentando Over-Issued CRLs

Neste modelo uma LCR é emitida antes que o período de validade da LCR emitida anteriormente expire.

Para o cenário ICP-Br poderíamos definir que cada LCR teria validade de uma hora, a cada 20 minutos uma nova LCR seria emitida e conseqüentemente teríamos 3 LCRs válidas em qualquer tempo dado. Com base no modelo proposto em [10] obtemos as taxas de requisição pra Over-Issued CRLs: $R_O(t) = (Nve^{-vt}) / ((O - 1) (1 - e^{-vl/O}) + 1)$. Neste caso teríamos picos de requisição de 18,9697 req/s, resultando em picos de consumo de banda de 794,3377 Kbytes/s. Um ganho de 65,85% em relação ao pico de consumo resultante do uso de LCRs básicas completas. O Gráfico 3 mostra o comportamento:

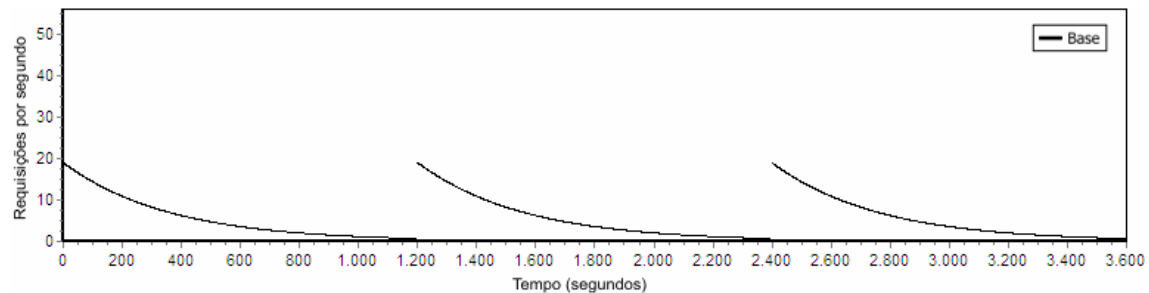


Gráfico 3. Taxa de requisição para Over-Issued CRLs

Quanto menor for o intervalo entre a emissão das LCRs menor será o pico de requisição. Ainda de acordo com [10], teremos um pico teórico mínimo, caso utilizássemos emissão contínua de LCRs: $R_O = \lim_{O \rightarrow 0} [Nv / ((O - 1) (1 - e^{-vl/O}) + 1)] = Nv / (vl + 1)$. Na prática isto não é viável. Emitindo continuamente Over-Issued CRLs teríamos um pico teórico mínimo de 5,0505 req/s.

A adoção deste modelo sobre uma infra-estrutura que já utilize emissão de LCRs básicas completas só requer que o agendamento da emissão de LCRs seja ajustado. Os verificadores não precisam sofrer qualquer alteração. Não existe ganho em relação à

quantidade de bytes que o cliente precisa transferir do repositório, pois ainda é necessário baixar a LCR inteira. O tempo de espera pela resposta do repositório pode diminuir, pois os picos de requisição serão minimizados.

4. Experimentando Over-Issued Segmented CRLs

Para promover melhoras na quantidade de bytes baixados pelo verificador, segmentar a distribuição de LCRs é uma alternativa. Em contra partida, segundo [10], caso seja utilizado um único repositório (servidor), a segmentação de LCRs não diminuí o pico de requisições. Para aproveitar os pontos positivos dos mecanismos Over-Issued CRLs e Segmented CRLs é possível fundi-los um único mecanismo, Over-Issued Segmented CRLs. Segundo [10], o pico da taxa de requisição para Over-Issued Segmented CRLs é dada por: $R_1(t) = (Nve^{-vt/s}) / ((O - 1)(1 - e^{-vl/sO}) + 1)$. Neste caso o pico teórico mínimo é dado por [10]: $Nvs / (vl + s)$. Assim como no modelo Over-Issued CRLs, é possível diminuir o pico de taxa de requisição aumentando a frequência de emissão das LCRs. Entretanto, aumentar o número de segmentos não reduz o pico de taxa de requisição.

Aplicando o modelo ao cenário ICP-Br, com 20 minutos entre as emissões de LCRs para cada segmento, 3 LCRs válidas em qualquer tempo dado e 3 segmentos, obtemos um pico de taxa de requisição igual a 23,7253 req/s. O pico obtido é levemente maior que o obtido com o cenário ICP-Br aplicado ao modelo Over-Issued CRL, mas isto pode ser compensado pelo fato das LCRs conterem apenas uma fração da lista inteira, portanto, são menores e de acesso menos custoso. O Gráfico 4 demonstra o comportamento do modelo.

Se cada segmento for emitido em um repositório (servidor) diferente, a taxa de requisição deve cair proporcionalmente. Se em uma situação hipotética e pouco provável de acontecer, os três segmentos, em repositórios diferentes, tivessem tamanhos iguais em um momento de pico igualmente distribuído, então o consumo de banda seria de proporções iguais. Para simular esta situação, é preciso definir para cada segmento o tamanho básico da LCR adicionado ao tamanho total das entradas da LCR. No cenário ICP-Br o tamanho básico da LCR é igual a 494 bytes, sobrando um total de $42.879 - 494 = 42.385$ bytes para as entradas na LCR completa. Então teríamos 865 entradas de 49 bytes distribuídos entre 3 segmentos. Para simulação teríamos dois segmentos de $494 + (288 \times 49) = 14.606$ bytes e um segmento de $494 + (289 \times 49) = 14.655$ bytes. Os dois primeiros repositórios teriam pico de consumo de banda igual a 112,8028 Kbytes/s, enquanto o terceiro repositório teria um pico de consumo de banda igual a 113,1813 Kbytes/s.

Para exemplificar as conseqüências do aumento do número de segmentos, se para o cenário ICP-Br utilizássemos 4 segmentos, o pico de taxa de requisição seria de 26,0726 req/s.

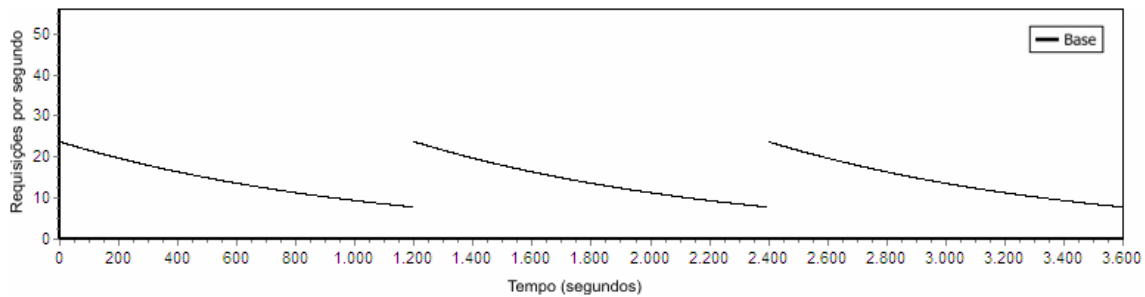


Gráfico 4. Taxa de requisição para Over-Issued Segmented CRLs

A adoção deste modelo implica no ajuste do agendamento por segmento de LCR, na definição de quantos segmentos serão necessários e o ajuste da extensão CDP dos certificados para apontar para um segmento. Uma característica deste modelo é que um segmento poder ter um crescimento diferente dos outros. Isto pode ser contornado com a utilização de uma extensão como a Redirect Pointer e LCRs de redirecionamento, como proposto em [11]. As aplicações verificadoras tratariam uma nova extensão.

5. Experimentando Delta-CRL

Segundo [12], o ganho considerável sobre a taxa de requisição da LCR base só acontece nos intervalos síncronos, ou seja, quando ela é emitida junto com uma Delta-CRL. A taxa de requisição da LCR base no intervalo síncrono é dada por [12]: $R(t) = Nve^{-vx(t+1)}$. Enquanto para o intervalo assíncrono a taxa é dada por: $R(t) = Nve^{-vt}$. A taxa de requisição da Delta-CRL também pode ser obtida pela mesma função, entretanto, neste caso, t é o tempo passado desde a emissão da última Delta-CRL válida.

Para o cenário ICP-Br, com uma Delta-CRL válida por 20 minutos, o pico de requisições para LCR base no intervalo síncrono é de 0,0025 req/s, no intervalo assíncrono de 1,9819 req/s e para Delta-CRL de 55,5556 req/s. Como proposto por [12], é possível calcular o tamanho médio da LCR base: $S_f = 494 + 49 \times r \times L_C/2$. Então teremos um tamanho médio de 32.150 bytes para a LCR base. O tamanho médio da Delta-CRL também pode ser calculado [12]: $S_\Delta = 494 + 49 \times r \times w$. Usando 20 minutos como janela, o tamanho médio da Delta-CRL resulta em 496 bytes. Para LCR base no intervalo síncrono o pico de consumo de banda seria de 0,0785 Kbytes/s, para a LCR base no intervalo assíncrono seria de 62,2256 Kbytes/s e para a Delta-CRL de 26,8666 Kbytes/s. O Gráfico 5 mostra o comportamento:

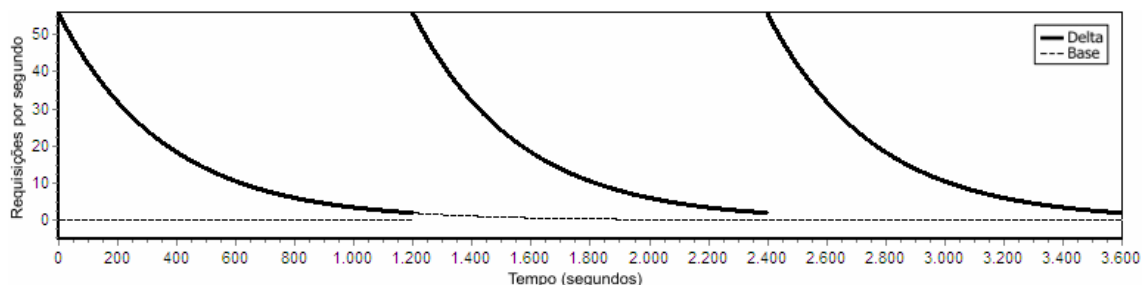


Gráfico 5. Taxa de requisição para Delta-CRL

A adoção deste modelo pela ICP-Brasil resultaria em um ganho de desempenho e disponibilidade de informações de revogação mais recentes, desde que a publicação da

LCR base fosse emitida em intervalos de muitas horas, 24 horas, por exemplo, para um bom aproveitamento do cache e diminuição dos picos de requisição. O modelo é suportado pela versão 2 do padrão X.509 para LCRs. Porém, isto não garante que todos os clientes verificadores já estejam preparados para processar as extensões específicas do uso de Delta-CRL.

6. Experimentando Sliding Window Delta-CRLs

A proposta do Sliding Window Delta-CRL [12] é fazer com que a janela da Delta-CRL tenha um tamanho fixo. Para que isso aconteça as LCRs base são sobre-emitidas e as Delta-CRL referenciam sequencialmente as LCRs base. A escolha do tamanho da janela é fundamental para o bom aproveitamento do modelo Sliding Window Delta-CRL. Para tal [12] propõe uma forma de calcular o tamanho ótimo de janela: $w = 1 - (1/O) + (1/v) \times \lg(((S_H + 0,5 \times S_E \times r \times L_C) \times v) / (S_E \times r))$. A manutenção do tamanho da janela deve acontecer com a frequência necessária para que o bom desempenho seja mantido. A taxa de requisição para Delta-CRL é obtida da mesma forma que obtemos a taxa em sistemas que utilizam emissão de LCR básicas completas [12]: $R_s(t) = Nve^{-vt}$. A taxa de requisição para LCR base pode ser obtida por: $R_{s\Delta}(t) = Nve^{-v(t+w)}$.

Para o cenário ICP-Br vamos considerar a média real de revogações da AC CertiSign SRF, que foi de 1,77 certificados revogados por dia de acordo com o levantamento. Para 10 certificados verificados por dia, $S_H=494$, $S_E=49$, $L_C=730$, $O=1$ e uma Delta-CRL com 20 minutos de validade obtemos uma janela ótima de 20 horas. O valor 1 foi atribuído a O, pois não é usada sobre-emissão de Delta-CRLs. O tamanho médio da LCR base seria de 32.150 bytes e o da Delta-CRL seria de 566 bytes. Com a Delta-CRL válida por 20 minutos e uma janela de 20 horas obtemos o pico de taxa de requisição muito próximo de zero para a LCR base, $7,6883 \times 10^{-86}$ req./seg, e o pico para a Delta-CRL seria o mesmo para o modelo de emissão de LCR básica completa. O pico de consumo de banda cairia para $(7,6883 \times 10^{-86} \times 32.150) + (55,5556 \times 566) = 30,7224$ Kbytes/s. O Gráfico 6 demonstra o comportamento:

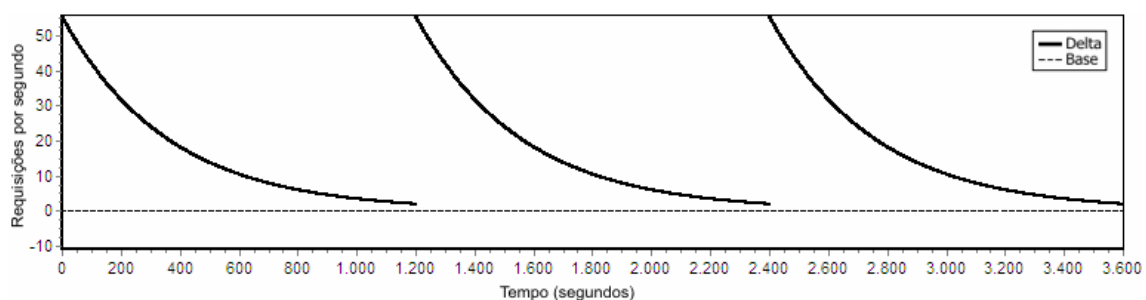


Gráfico 6. Taxa de requisição para Sliding Window Delta-CRLs

A adoção deste modelo para ICP-Brasil tem um impacto considerável, pois o padrão v2 das LCRs não contempla [3, 9] a estrutura necessária para implementá-lo. A utilização de Sliding Window Delta-CRL pode representar um grande ganho de desempenho, mas seria necessário um esforço da parte das aplicações verificadoras e dos emissores das listas para se adequarem a este modelo. A não conformidade com os padrões torna o modelo um forte candidato a não utilização.

7. Experimentando Over-Issued Delta-CRLs

Assim como o modelo Sliding Window Delta-CRL, este modelo baseia-se no uso de Delta-CRL, porém, neste caso, estas também são sobre-emitidas. Para este modelo teremos mais de uma LCR válida em qualquer tempo dado. A taxa de requisição para as Delta-CRLs pode ser obtida pela mesma função utilizada em sistemas que utilizam LCR sobre-emitidas, mas não utilizam Delta-CRLs. A taxa de requisição para LCR base pode ser obtida pela função [12]: $R_b(t) = (Nve^{-(t+w+1/O-1)v}) / ((O-1)(1 - e^{-v/O}) + 1)$.

Para o cenário ICP-Br consideramos a média de 1,77 certificados revogados por dia, 10 certificados verificados por dia, $S_H=494$, $S_E=49$, $L_C=730$, $O=3$, uma Delta-CRL com 20 minutos de validade e uma janela ótima de 20 horas. Teríamos um pico extremamente próximo de zero para a LCR base, $2,0628 \times 10^{-83}$ req/s e para Delta-CRL o pico seria de 23,7253 req/s. O pico de consumo de banda seria de 13,1202 Kbytes/s. O Gráfico 7 mostra o comportamento da taxa da Delta-CRL para esta situação:

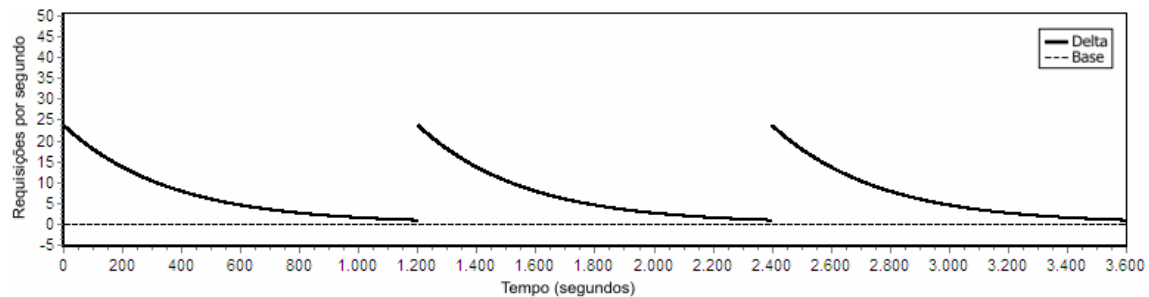


Gráfico 7. Taxa de requisição para Over-Issued Delta-CRLs

As mesmas considerações sobre o impacto da adoção do Sliding Window Delta-CRL, também [3, 9] são válidas para este modelo. Um outro modelo que compartilha das mesmas restrições é o Over-Issued Delta-CRL with Distribution Points [13].

8. Resultados

A Tabela 1 mostra os resultados para o cenário ICP-Br:

Tabela 1. Resultados das avaliações

Modelo	Base (req/s)	Base (Kbytes/s)	Delta (req/s)	Delta (Kbytes/s)
CRL	55,5556	2326,3365	-	-
Over-Issued CRLs	18,9697	794,3377	-	-
Over-Issued Segmented CRLs	23,7253	113,1813	-	-
Delta-CRLs	1,9819	62,2256	55,5556	26,8666
Sliding Window Delta-CRLs	$7,68 \times 10^{-86}$	$2,47 \times 10^{-84}$	55,5556	30,7224
Over-Issued Delta-CRLs	$2,06 \times 10^{-83}$	$6,63 \times 10^{-82}$	23,7253	13,1202

9. Conclusão e Trabalhos Futuros

A melhor solução deve balancear a necessidade de informações recentes, um desempenho aceitável e o baixo impacto na infra-estrutura já existente. O modelo Over-Issued Segmented CRLs pode ser utilizado em harmonia com o ambiente atual da ICP-Brasil, apresentou ganhos de desempenho e pode ser aplicado imediatamente. E mesmo sem a utilização de artifícios para redimensionamento dinâmico de LCRs traria

benefícios de desempenho. Embora o modelo Delta-CRL possa proporcionar melhor desempenho, aplicações que lidam com LCRs básicas poderiam ter que sofrer adaptações. Os mecanismos Sliding Window Delta-CRLs e Over-Issued Delta-CRLs não são suportados pelos padrões [3].

Este trabalho tem um perfil prático inédito entre os trabalhos que tratam do mesmo tema [9, 10, 11, 12, 13, 14, 15], explorando um ambiente real e amplo. Além de expor informações que certamente servirão de base para uma reavaliação das práticas da ICP-Brasil, procura apontar uma solução viável e de baixo impacto. Deixa margem também para futuras análises da ICP-Brasil utilizando outros mecanismos.

Referências

- [1] Medida Provisória nº2.200-2, de 24 de agosto de 2001
- [2] Resolução nº6, de 22 de novembro de 2001
- [3] ITU. X.509. ITU-T Recommendation, junho de 1997
- [4] Declaração de Práticas de Certificação da AC Raiz da ICP-Brasil
- [5] Módulo Security Solutions S.A. 7ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, Brasil, 2001
- [6] Módulo Security Solutions S.A. 8ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, Brasil, 2002
- [7] Módulo Security Solutions S.A. 9ª Pesquisa Nacional de Segurança da Informação. Rio de Janeiro, Brasil, 2003
- [8] Housley, R.; Ford, W.; Polk, W.; Solo, D. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. RFC 2459. 1999
- [9] Arnes, André. Public Key Certificate Revocation Schemes. Tese para o Departamento de Telemática, Queen's University, Ontário, Canadá, 2000
- [10] Cooper, David A. A model of certificate revocation. Annual Computer Security Applications Conference, p.256–264, 1999
- [11] Adams, Carlisle; Zuccherato, Robert. A General, Flexible Approach to Certificate Revocation. Entrust Technologies White Paper, 1998
- [12] Cooper, David A. A More Efficient use of Delta-CRLs. IEEE Symposium on Security and Privacy, p.190-202, 2000
- [13] Rojanapasakorn, Aradee; Sathitwiriawong, Chanboon. A Performance Study of Over-Issuing Delta-CRLs with Distribution Points. International Conference on Advanced Information Networking and Application (AINA'04)
- [14] Rivest, Ronald. Can We Eliminate Certificate Revocation Lists?. Financial Cryptography, v.1465, p.178-183, 1998
- [15] McDaniel, Patrick; Rubin, Aviel. A Response to "Can We Eliminate Certificate Revocation Lists?". Technical Report 99.8.1, Laboratórios da AT&T, 2000