

# Uso de Webservices Criptográficos a partir de Dispositivos Móveis

Daniel Melo<sup>1</sup>

<sup>1</sup>Instituto de Informática – Universidade Federal de Goiás  
Alameda Palmeiras, Quadra D, Câmpus Samambaia  
CEP 74690-900 – Goiânia – GO – Brasil

danielmelo@inf.ufg.br

**Abstract.** *This meta-paper describes the style to be used in articles and short papers for SBC conferences. For papers in English, you should add just an abstract while for the papers in Portuguese, we also ask for an abstract in Portuguese (“resumo”). In both cases, abstracts should not have more than 10 lines and must be in the first page of the paper.*

**Resumo.** *A criptografia é uma técnica muito conhecida por usuários de software mais experientes, mas pouco difundida dentre os demais. O desenvolvimento das ferramentas e técnicas não tem sido suficiente para assegurar a sua adoção por grandes grupos de usuários. Isso se deve, em grande parte, à dificuldade de uso dessas ferramentas. Neste trabalho avaliamos o cenário de adoção da criptografia e propomos um modelo mais próximo da experiência do usuário final, utilizando dispositivos móveis como facilitadores das experiências ligadas à segurança da comunicação que usam essa tecnologia.*

## INTRODUÇÃO

Um dos grandes desafios das aplicações modernas está na sua capacidade de manter a segurança dos dados de seus usuários. Um dos pilares da segurança da informação é a confidencialidade [REF1], que é manter aquilo que é privado acessível somente a quem é de direito, identificando de forma inequívoca as partes envolvidas e suas ações no seu sistema de informação. Outro conceito importante é o da integridade, que busca afirmar com precisão se determinado conteúdo se mantém sem modificações inapropriadas[REF1].

Um recurso voltado para essas necessidades é a criptografia, capacidade de mascarar uma mensagem de tal forma que somente seja legível pelo destinatário. Também traz a possibilidade de assinar digitalmente os conteúdos das mensagens, sendo possível verificar posteriormente quem assinou e se o conteúdo não sofreu alteração depois disso. O uso crescente de ferramentas sociais para comunicação entre as pessoas em ambientes diversificados traz a necessidade da garantia de privacidade de forma efetiva e fácil de usar.

Apesar do uso de tais técnicas de segurança ser conhecido há muitos anos [REF3] (com a criptografia datando de 1900 A.C[REF9] e a criptografia assimétrica de 1975 [REF2] ) - ele ainda é de difícil compreensão e uso para usuários finais. Visto que a facilidade de uso precede uma adoção em massa de qualquer tecnologia [REF4], existe necessidade de desenvolver formas mais simples de uso para potencializar ações de segurança da informação.

Este artigo faz uma análise do uso atual de criptografia de chaves assimétricas com PGP para troca de mensagens em algumas ferramentas e propõe um formato simplificado da gestão dos recursos privados usando webservices criptográficos oferecidos em dispositivos móveis. O objetivo principal é simplificar seu uso pelo usuário final e potencializar o uso de criptografia fim a fim.

## **LIMITAÇÕES DE COMUNICAÇÃO SEM CRIPTOGRAFIA FIM A FIM**

A criptografia fim a fim é definida pela implementação de técnicas que garantam que somente o remetente e o destinatário tem acesso às mensagens trocadas, sendo computacionalmente inviável que alguém leia as mensagens, seja por meio de interceptação, seja por acesso indevido aos dispositivos físicos envolvidos. Esse tipo de criptografia não tem sido historicamente desenvolvida com foco no usuário final [REF5].

Parte significativa da confidencialidade na troca de mensagens reside atualmente na criptografia das mensagens em trânsito através da rede. Isso é feito usando algum protocolo baseado em SSL/TLS, sigla para os padrões Secure Socket Layer e Transport Layer Security [REF6]. São exemplos o HTTPS, SMTPS, para troca de hipertexto e e-mail, respectivamente. Essa estratégia busca proteger as partes envolvidas de ataques contra o sigilo das mensagens, uma vez que o conteúdo interceptado de forma indevida durante o trânsito se torna ilegível para o atacante. Também torna computacionalmente complexo introduzir nas mensagens conteúdo não legítimo.

Apesar da elevada proteção contra interceptação, estes meios não buscam resolver o problema de somente o remetente e o destinatário da mensagem poderem lê-la. No caso de provedores de e-mail comerciais, como o Gmail, Yahoo Mail e Outlook Mail o mantenedor do serviço ainda tem acesso ao conteúdo das mensagens à revelia da vontade de sigilo do usuário[REF8]. Cria-se a necessidade de confiar no provedor de e-mail para trocar uma mensagem sigilosa, o que não é suficiente em contextos sensíveis.

A criptografia assimétrica propõe um modelo de solução para este problema. Cada usuário gera um par de chaves criptográficas, sendo uma de propósito privado e a outra pública. A chave privada é usada para assinar e descriptografar as mensagens. A chave pública, por sua vez é usada para verificar assinaturas e criptografar as mensagens, que só poderão ser lidas por quem possuir a chave privada equivalente. Isso cria um mecanismo onde somente o destinatário pode ler as mensagens, promovendo a confidencialidade. Além disso, a capacidade de assinatura provê o recurso de não-repúdio e integridade da comunicação. Se esses recursos forem empregados na troca de mensagens temos um exemplo de criptografia fim a fim.

O chaveiro criptográfico em tem como funções a proteção das chaves privadas, a importação de chaves públicas alheias, revogação de chaves comprometidas e configuração do nível de confiança. Sendo a camada responsável por estas tarefas, está fortemente ligado à facilidade de uso das chaves pelo usuário final. O chaveiro desempenha a função crucial de proteção das chaves privadas por meio de senha. A solução adotada em implementações como o GnuPG cria um chaveiro na estação de trabalho do usuário durante a instalação, que pode então ser usado diretamente por meio de linha de comando ou acessado por através de bibliotecas específicas por softwares de terceiros.

## First Page

The first page must display the paper title, the name and address of the authors, the abstract in English and “resumo” in Portuguese (“resumos” are required only for papers written in Portuguese). The title must be centered over the whole page, in 16 point boldface font and with 12 points of space before itself. Author names must be centered in 12 point font, bold, all of them disposed in the same line, separated by commas and with 12 points of space after the title. Addresses must be centered in 12 point font, also with 12 points of space after the authors’ names. E-mail addresses should be written using font Courier New, 10 point nominal size, with 6 points of space before and 6 points of space after.

The abstract and “resumo” (if is the case) must be in 12 point Times font, indented 0.8cm on both sides. The word **Abstract** and **Resumo**, should be written in boldface and must precede the text.

## CD-ROMs and Printed Proceedings

In some conferences, the papers are published on CD-ROM while only the abstract is published in the printed Proceedings. In this case, authors are invited to prepare two final versions of the paper. One, complete, to be published on the CD and the other, containing only the first page, with abstract and “resumo” (for papers in Portuguese).

## Sections and Paragraphs

Section titles must be in boldface, 13pt, flush left. There should be an extra 12 pt of space before each title. Section numbering is optional. The first paragraph of each section should not be indented, while the first lines of subsequent paragraphs should be indented by 1.27 cm.

## Subsections

The subsection titles must be in boldface, 12pt, flush left.

## Figures and Captions

Figure and table captions should be centered if less than one line (Figure 1), otherwise justified and indented by 0.8cm on both margins, as shown in Figure 2. The caption font must be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

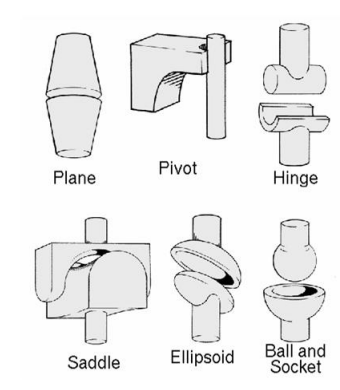
In tables, try to avoid the use of colored or shaded backgrounds, and avoid thick, doubled, or unnecessary framing lines. When reporting empirical data, do not use more decimal digits than warranted by their precision and reproducibility. Table caption must be placed before the table (see Table 1) and the font used must also be Helvetica, 10 point, boldface, with 6 points of space before and after each caption.

## Images

All images and illustrations should be in black-and-white, or gray tones, excepting for the papers that will be electronically available (on CD-ROMs, internet, etc.). The image resolution on paper should be about 600 dpi for black-and-white images, and 150-300 dpi for grayscale images. Do not include images with excessive resolution, as they may take hours to print, without any visible difference in the result.



**Figure 1. A typical figure**



**Figure 2. This figure is an example of a figure caption taking more than one line and justified considering margins mentioned in Section 6.**

## References

Bibliographic references must be unambiguous and uniform. We recommend giving the author names references in brackets, e.g. [Knuth 1984], [Boulic and Renault 1991], and [Smith and Jones 1999].

The references must be listed using 12 point font size, with 6 points of space before each reference. The first line of each reference should not be indented, while the subsequent should be indented by 0.5 cm.

## References

Boulic, R. and Renault, O. (1991). 3d hierarchies for animation. In Magnenat-Thalmann, N. and Thalmann, D., editors, *New Trends in Animation and Visualization*. John Wiley & Sons Ltd.

Knuth, D. E. (1984). *The T<sub>E</sub>X Book*. Addison-Wesley, 15th edition.

Smith, A. and Jones, B. (1999). On the complexity of computing. In Smith-Jones, A. B., editor, *Advances in Computer Science*, pages 555–566. Publishing Press.

**Table 1. Variables to be considered on the evaluation of interaction techniques**

	Chessboard top view	Chessboard perspective view
Selection with side movements	6.02 $\pm$ 5.22	7.01 $\pm$ 6.84
Selection with in- depth movements	6.29 $\pm$ 4.99	12.22 $\pm$ 11.33
Manipulation with side movements	4.66 $\pm$ 4.94	3.47 $\pm$ 2.20
Manipulation with in- depth movements	5.71 $\pm$ 4.55	5.37 $\pm$ 3.28