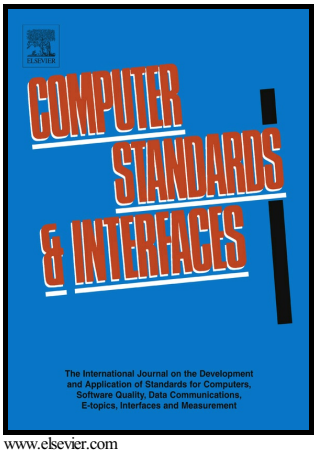
Policy-controlled signatures and their applications

Pairat Thorncharoensri, Willy Susilo, Yi Mu



www.elsevier.com

PII: S0920-5489(16)30062-9
DOI: http://dx.doi.org/10.1016/j.csi.2016.08.005
Reference: CSI3126

To appear in: *Computer Standards & Interfaces*

Received date: 16 February 2016
Revised date: 29 June 2016
Accepted date: 11 August 2016

Cite this article as: Pairat Thorncharoensri, Willy Susilo and Yi Mu, Policy-controlled signatures and their applications, *Computer Standards & Interfaces* http://dx.doi.org/10.1016/j.csi.2016.08.005

Policy-controlled Signatures and Their Applications[☆]

Pairat Thorncharoensri[a,*], Willy Susilo[b], Yi Mu[b]

[a] *Department of Computer Science, Faculty of Science, King Mongkut's Institute of Technology Ladkrabang, Chalongkrung Rd. Ladkrabang, Bangkok, 10520, Thailand*
[b] *Centre for Computer and Information Security, School of Computer Science and Software Engineering, University of Wollongong, Wollongong, NSW 2522, Australia*

Abstract

In this paper, we present a new cryptographic primitive called "policy-controlled signatures". In this notion, a signer can sign a message and attach it with some policies. Only a verifier who satisfies the policies attached can verify the authenticity of the message. This type of signature schemes has many applications, in particular to deal with sensitive data, where the signer does not want to allow anyone who is unauthorized to verify the authenticity of the messages. The notion of policy-controlled signatures resembles some similarities with designated verifier signatures, as it can also be used to *designate* a signature to multiple recipients. Nevertheless, we shall demonstrate that the notion of policy-controlled signatures generalize the notion of designated verifier signatures. A concrete scheme that is secure in our model is also provided. Furthermore, we also present an extension to "universal policy-controlled signature". In this extended notion, we combine the idea of universal designated verifier signatures with policy-controlled signatures to allow more flexible delegations. We also provide a concrete scheme that is secure in our model.

[☆]This paper is an extended version of the conference paper: P. Thorncharoensri, Y. Mu and W. Susilo. Policy-controlled Signature. Eleventh International Conference on Information and Communications Security (ICICS 2009), Lecture Notes in Computer Science 5927, pp. 91 - 106, Springer-Verlag, 2009. This paper has a revised scheme and its extension, together with their proofs. This work is partially supported by ARC Linkage Project Grant LP0667899.

[*]Corresponding author

Email addresses: pt78@uow.edu.au (Pairat Thorncharoensri), wsusilo@uow.edu.au (Willy Susilo), ymu@uow.edu.au (Yi Mu)