SCHOOL OF COMPUTER SCIENCE AND SOFTWARE ENGINEERING
MONASH UNIVERSITY

TECHNICAL REPORT 2004/154

XML Signature Extensibility Using Signer-Specified Custom Transforms

L Bull and D McG Squire

ABSTRACT

In this paper we further investigate the extensibility of the XML Signature using custom transforms to achieve additional functionality. We introduce a new custom transform and XML Signature structure that overcomes fragment scope restriction in the XML signature Core Validation process. This enables the XML Signature framework to support a grouping extraction policy for Content Extraction Signatures. We also show how to embed a custom transform in the signature itself, and discuss the implications of this approach. We highlight a possible vulnerability in the existing XML Signature Core Validation process when using custom transforms, and suggest an extension to the XML Signature standard to remedy this. We propose processing rules that any implementation should obey.