

# Internet Attribute Certificate Profile for Authorization - An Analyses

Ruud Verbij

*Abstract*—**ABSTRACT**

*Index Terms*—**Keywords**

## I. INTRODUCTION

Below is a list of 8 RFC assignments. Read and study the RFC (skip the very technical stuff such as ASN.1, focus on cryptographic and PKI matters). Then give a summary of the RFC on a high level, addressing the following issues:

- 1) How does this RFC fit in the entire PKI picture? Who is expected to use this RFC, what for, and how?
- 2) What are the security requirements outlined in this RFC? What security problems does it attempt to solve? What (cryptographic) attacks does it defend against?
- 3) Give an overview of the solution that the RFC proposes. How is cryptography used in Cryptography 2 version 1.0, May 13, 2013 meeting the security requirements, solving the security problems, defending against the attacks?