A Critical View on RFC 3647

Klaus Schmeh

cv cryptovision gmbh, Munscheidstr. 17,
45886 Gelsenkirchen, Germany
klaus.schmeh@cryptovision.com

Abstract. A Certification Practice Statement (CPS), as well as one or several Certificate Policies (CP) are important parts of a Public Key Infrastructure. The by far most important source of information for writing a CPS or CP was developed by an IETF working group and was published as RFC 3647 [1]. RFC 3647 can be thought of as a generic instruction set for creating a CPS and a CP. Yet, experience shows that working with RFC 3647 can be quite difficult. This is due to some fundamental issues, but also due to some shortcomings and faults in the standard. In addition, it is difficult to use RFC 3647 for a CPS/CP that is used outside the US. This paper names the main problems that a CPS/CP author has to face when following RFC 3647. It discusses possible solutions and reveals why the development of a new standard would be appropriate.

Keywords: PKI, Certification Practice Statement, CPS, Certificate Policy, CP.

1 Introduction

RFC 3647 is the successor of RFC 2527 [2] and can therefore be regarded as a second version document. RFC 3647 is an Informational RFC, which implies that it has no official standard status. Anyway, it will be called a standard in this document, because it is a de-facto standard (obviously, for a paper document the existence of a well-specified standard is less important than for a software solution). Virtually every CPS/CP author uses RFC 3647 as a source of information. To my knowledge there are no relevant alternatives to RFC 3647 today.

The core of a CPS or CP according to RFC 3647 is a so-called „Set of Provisions“. RFC 3647 lists about 58 provision names that may or may not be used by a CPS/CP author. The provisions are grouped into nine chapters. In addition to the provision names, RFC 3647 also describes details about how a provision might look like in an actual CPS/CP. Yet, RFC 3647 doesn't list any provisions itself, nor does it require that certain provision types are present in a CPS/CP. RFC 3647 therefore can be thought of as a toolkit for CPS/CP documents with the provisions as generic building blocks.

Most CPS/CP authors don't keep exactly to the structure proposed in RFC 3647. Usually, RFC 3647 is only used as a rough guideline and as a general source of information. In my view, this is an unlucky situation, because it would have major advantages to have CPS/CP documents that are structured in the same way and that

J. Lopez, P. Samarati, and J.L. Ferrer (Eds.): EuroPKI 2007, LNCS 4582, pp. 369–374, 2007.

have an analogous content. This would make CPS/CP comparisons a lot easier, and, most of all, would provide for easy policy mapping like it is described in the X.509v3 and the PKIX standards.

One reason for this undesired situation is, of course, the complexity of the PKI topic itself. Yet, RFC 3647 is in my view more complex than necessary, and it has a number of serious disadvantages. The scope of this paper is to name the problems that arise when using RFC 3647. All the problems mentioned have a close relation to practice. This paper is based on experience gathered in more than 20 PKI projects with about a dozen CPS/CP documents.

2 Structure Problems

The structure RFC 3647 suggests for a CPS/CP document is not optimal. In my view, an RFC 3647 set of provisions doesn't provide an easy, intuitive way to find the information the reader is looking for. I see the following reasons for this:

- It is usually considered best-practice to group the description of an IT system into three parts: components, roles, and processes. In many cases one or two additional parts, like "Introduction" or "Policy Issues", may be useful. Yet, RFC 3647 follows a completely different approach. It uses a nine chapter structure: "Introduction", "Publication and Repository Responsibilities", "Identification and Authentication", "Certificate Life-Cycle Operational Requirements", "Facility, Management, and Operational Controls", "Technical Security Controls", "Certificate, CRL, and OCSP Profiles", "Compliance Audit and Other Assessment", and "Other Business and Legal Matters". In my view, it is a lot harder to find the desired information in this structure than it is in a conventional components-roles-processes document.
- Some of the nine chapters recommended in RFC 3647 are in practice very short or even empty. E.g., chapters 2 and 8 don't have subchapters and are therefore usually quite short. Chapter 9 is usually very short, too, because most of its provisions are not relevant in practice. On the other hand, chapters 3, 4, 6 and 7 may grow quite comprehensive. A components-roles-processes structure would avoid such differences in length.
- As there is no dedicated chapter for processes, it is not possible to get an overview on the PKI processes specified by a RFC 3647 document at first sight. Instead, process descriptions are spread to several chapters (4, 5 and 6), which is not very intuitive.
- The situation with roles is similar as with processes. It is not intuitively clear, where roles are described. To be precise, RFC 3647 not even mentions the word "role". Instead, it uses the term "participants". Participants can be described as a part of the introduction subchapter. I consider this a major shortcoming, because roles are important in a PKI and should not be presented as introductory information, but as a substantial part of a CPS/CP.
- In RFC 3647, PKI components are covered even worse than PKI processes and PKI roles. There is simply no provision at all, that is designed to contain a description of all relevant components. Thus, a CPS/CP author has to hide the complete PKI architecture description in the introduction subchapter named "Overview", which doesn't grant this topic the importance it deserves.