

RFC 3280 の UTF8String 問題についての注意喚起

2003 年 12 月 3 日

情報処理振興事業協会

日本ネットワークセキュリティ協会

要旨：PKI における UTF8String 問題の存在を指摘しつつ、拙速な対応は控えるよう促す。
2004 年 1 月 1 日以降、認証局は無理に UTF8String の公開鍵証明書を発行する必要はない。
第 58 回 IETF 会合において、UTF8String の導入期限は、実質的に先送りされた。

1. 背景

PKIの基本的な標準文書であるRFC 3280 には、「2003 年 12 月 31 日より後に発行するすべての公開鍵証明書について、以下の場合を除いてDirectoryStringをUTF8String¹でエンコードしなければならない」(4.1.2.4 Issuer)と記述されている。

- ・ UTF8String に移行するための Name Rollover 証明書を発行する場合。
- ・ 認証局証明書の subject が、その認証局が発行するすべての証明書の発行者と一致している場合。ただし、両者のエンコーディングが一致している必要はない。また両者とも空であってはならない。

この記述は、前の版の標準文書である RFC 2459(1999 年 1 月)当時から存在しており、これを改訂した現行 RFC 3280 においても、この記述が残ってしまったので、問題の期限が迫っている。

2. UTF8String 問題とは？

しばしば、以下の 2 つの論点が指摘される。

(1) 2004 年になったとき、認証局はどのようにすればよいのか？

(2) UTF8String と他のエンコーディングによる文字列を比較する方法は？

まず、「2004 年になったとき、認証局はどうすればよいのか？」という問題には、以下の疑問が含まれる。

- ・ 証明書を再発行する必要があるのか？
- ・ 証明書や CRL の発行者はどうすればよいのか？

次に、UTF8String と他のエンコーディングによる文字列の比較方法について、例を示せば次のようになる。

- ・ UTF8:'AAA' と Printable:'AaA' は、同値と見なしてよいのか？

さらに、UTF8String の実装上の問題として、以下の事項が挙げられる。

- ・ UTF8String 対応アプリケーションが少ない (UTF8String を用いた証明書を正しく処理できる対応製品が少ない。)
- ・ UTF8String と他のエンコーディングとの文字列比較方法が不明確 (UTF8String をバイナリ比較してしまっている実装がいくつかある。)

¹ UTF8(Unicode Transformation Format 8)によってエンコードされた文字列。

これらの問題のうちいくつかについては、その解が関連する仕様に示されているが、いずれにせよ解釈を誤る可能性がある。

3. IETF の PKIX WG における動向

RFC 3280 における問題の記述箇所については、著者らが削除し忘れたものであった。これは、第 58 回 IETF 会合において著者の一人である Tim Polk 氏との議論において判明した。そのため、今後、他のエンコーディングとの比較規則を明確化することとなった。

- ・ UTF8String における比較規則の標準化作業を憲章 (Charter) 中に掲げる。
- ・ “LDAPv3 DN strings for use with PKIs” (draft-ietf-pkix-dnstrings-02.txt) の策定。

また、上記以外にも、の新しい I-D (インターネットドラフト) 文書が提案される予定である。

The only new work item is a name comparison spec (to address international name issues), an initial draft of which is slated for the Seoul meeting.

現実問題として、UTF8String 導入の期限 (2003 年 12 月 31 日) は、先送りされることとなった。

4. 現状における対応

UTF8String 問題は、簡単に解決する問題ではない。まずは、曖昧さが残っている仕様を明確化することに注力される。

したがって、当面、無理に UTF8String の公開鍵証明書を発行する必要はない。単に仕様で策定されているからという理由によって、このような公開鍵証明書を発行しても、いたずらに混乱を招くだけで利点は無い。製品によっては、まだ対応していない可能性がある。

5. 公開鍵証明書

そこで、どのような公開鍵証明書を発行したらよいのであろうか? 下表を参照していただきたい。

表 公開鍵証明書の項目のエンコーディング

認証局証明書の subject	発行する証明書の発行者	発行する証明書の subject
PrintableString	PrintableString	PrintableString または UTF8String
UTF8String 以外の エンコーディング X	エンコーディング X	エンコーディング X または UTF8String
UTF8String	UTF8String	任意

整合性

ここで「認証局証明書の subject」と「発行する証明書の発行者」の整合性を保つことが重要である。「発行する証明書の発行者」情報の「PrintableString」と「エンコーディング X」について、むやみに UTF8String にしてはならない。

6. 注意事項

既に認証局を運用しており、自身の認証局証明書を発行している場合、新規に UTF8String としてエンコードした公開鍵証明書を発行する必要はない。今まで使っていた認証局証明書を使うことができる。また、エンドエンティティ用の証明書については、発行者を今まで使っていたエンコード方法を使い続けるようにするのが無難である。

新たに認証局証明書を発行する場合、UTF8String と PrintableString のいずれのエンコードによる認証局証明書も発行できる。ただし、アプリケーションが UTF8String を扱えるかを確認する必要がある。(例：Web サーバー、VPN 装置等のサーバー製品群および Web ブラウザ、S/MIME 対応メーラー等のクライアントアプリケーション製品群。)エンドエンティティ用の証明書については、発行者を認証局証明書と同じ手法でエンコードする必要がある。

‘country’については、PrintableString のままとする。‘c=JP’のように‘country’部分に限っては例外的に PrintableString のままエンコードしなければならない。この他にも、いくつか UTF8String でエンコードしてはいけない項目もあるので注意を要する。

7. 今後の展開

IETF の PKIX WG において、UTF8String の名前比較規則 (DN Matching Rule) についての仕様を策定することとなった。これについては、次回の第 59 回 IETF 会合までに仕様案が提出される予定である。

RFC 3280 の改訂について、UTF8String 問題に関する部分の記述が改訂される見込みであり、これについても次回の第 59 回 IETF 会合までにその仕様案が提出される予定であるので、注目する必要がある。ちなみに次回の第 59 回 IETF 会合は、大韓民国のソウルにおいて、2004 年 2 月 28 日から 3 月 5 日まで、開催される予定である。

8. 参考文献

[RFC 3280] Housley, R., Polk, T, Ford, W. and Solo, D., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 3280, April 2002.

[RFC 2459] Housley, R., W. Ford, W. Polk and D. Solo, "Internet X.509 Public Key Infrastructure: Certificate and CRL Profile", RFC 2459, January 1999.

情報処理振興事業協会,

「GPKIアプリケーション実装ガイド報告書」,
<http://www.ipa.go.jp/security/fy14/development/pki/interop.html>, p.144, 2002年3月