

-----Message d'origine-----

De : peter.nobs@post.ch [<mailto:peter.nobs@post.ch>]  
Envoyé : vendredi, 11. août 2006 17:39  
À : \_BAKOM-DigSig  
Cc : reto.muellhaupt@post.ch; veronika.stadelmann@post.ch;  
barbara.oechslin@post.ch  
Objet : Änderungsentwurf SR 943.032.1; Anhörung

Änderungsentwurf der technischen und administrativen Vorschriften über  
Zertifizierungs- Dienste im Bereich der elektronischen Signatur (SR  
943.032.1); Anhörung der betroffenen Kreise Stellungnahme der Post

Sehr geehrte Damen und Herren

Wir beziehen uns auf Ihr Schreiben vom 23. Juni 2006 in der oben erwähnten  
Angelegenheit und erlauben uns, Ihnen nachfolgend die Bemerkungen unseres  
Fachdienstes zukommen zu lassen:

Ad. Ziffer 3.4.2 c)

Das Feld keyUsage sollte "mindestens" anstatt "exakt" das bit 1 gesetzt  
haben. Es soll damit möglich werden, weitere bits zu setzen. Die  
Einschränkung der keyUsage führt heute lediglich dazu, dass keine  
Applikation mit dem qualifizierten Zertifikat umgehen kann.

Das Feld Transaktionslimite bringt in der aktuellen Form keinen Nutzen,  
sondern sorgt eher für Verwirrung. Dieses sollte optional anwendbar gemacht  
werden. Dies bedeutet, dass der CSP entscheiden soll, ob das  
Feld im Zertifikat eingetragen wird oder nicht.

Wir hoffen, Ihnen damit zu dienen.

Freundliche Grüsse  
Peter Nobs

Die Schweizerische Post  
Rechtsdienst  
Viktoriastrasse 21  
3030 Bern

Telefon 031 338 63 80  
Fax 031 338 09 59  
E-Mail peter.nobs@post.ch