P.	Ch.	Topic	Comment
10 ff	3.	Qualified Certificate	General comment: The latest versions of the ordinance (VZertES) and the technical and administrative prescriptions (TAV) to the Swiss signature law (ZertES) allow qualified signatures to be remote signatures, i.e. the application of a qualified signature at a server. A possible authentication method to access such a service is the usage of a SuisseID authentication certificate. It also has to be considered that the vast majority of the SuisseID-enabled applications do not require a qualified signature. These explanations show that a qualified certificate is not a necessity. Therefore, it should be optional on a SuisseID token (smartcard or USB-stick). Only the authentication certificate should be mandatory.
7/8	3.3.1	SuisseID number	General comment: Section 3.3.1 describes the structure of the SuisseID number which is included as Serial Number in the Distinguished Name. This number can be recognized as such only in the (closed) SuisseID context (e.g. by checking the policy information). In an open international environment the SuisseID number cannot unfold its full potential the way it is now designed. A unique prefix before the SuisseID number would enhance the recognition of the SuisseID number. (The optional Microsoft UPN for Windows Logon in authentication certificates containing the SuisseID number on the other hand might be unique but is only for use in a very limited area.) It should also be considered to extend the SuisseID numbering system and to allow identifiers which dedicate the certificate holder as part of an organization. This would make the identification of the organization (company) involved very simple. Therefore, such an identifier system would enhance the usage of SuisseID certificates for B2B (and also B2G) purposes. Some thoughts on this can be found in the CEN CWA 16036:2009

P.	Ch.	Topic	Comment
			"cyber-identity - Unique Identification Systems for Organizations and Parts Thereof" (ftp://cenftp1.cenorm.be/PUBLIC/CWAs/Cyber_Identity/CWA_CyberIdentity.pdf).
11	3.4.4 / 3.4.5	QC Format Extensions	Technical comment: The technical and administrative prescriptions (TAV) to ZertES mention in section 3.4.2 c) regarding extensions of qualified certificates the possible insertion of a "QcLimitValue" in the "qcStatement" extension. The QcLimitValue contains a "transaction limit, if necessary". (Based upon ZertES Art. 7.2 c) The SuisseID specification should make a recommendation if the inclusion of a QcLimitValue is useful or not. If yes, it should state what the recommended monetary value should be.
30 ff	4.6.3	Assertion Attributes	General comment: An attribute like „isOver18“ is a) a very static attribute and b) causes few or no problems concerning privacy. This kind of attribute could therefore be written directly into the SuisseID certificates instead of just being stored in the IdP databases. This setup would allow a validating party – e.g. an online whisky shop – to check this information directly and would therefore spare it the considerable technical overhead of IdP-lookups.
77	Annex C	Abreviations	Editorial comment: TAV stands for “Technische und administrative Vorschriften“ (prescriptions), not for „Technische Ausführungsverordnung“ (ordinance).