AMENDMENTS TO DIGITAL SIGNATURE ACT

2000 GENERAL SESSION

STATE OF UTAH

Sponsor: David H. Steele

AN ACT RELATING TO DIGITAL SIGNATURES; AMENDING PROVISIONS MANDATING THAT THE DIVISION OF CORPORATIONS AND COMMERCIAL CODE BE A CERTIFICATION AUTHORITY AND RELATED PROVISIONS; AMENDING THE EXEMPTION OF A CERTIFICATION AUTHORITY FROM THE AUDIT REQUIREMENT; AND MAKING CONFORMING AMENDMENTS.

This act affects sections of Utah Code Annotated 1953 as follows:

AMENDS:

46-3-104, as repealed and reenacted by Chapter 205, Laws of Utah 1996

46-3-202, as last amended by Chapter 205, Laws of Utah 1996

Be it enacted by the Legislature of the state of Utah:

Section 1. Section **46-3-104** is amended to read:

46-3-104. Role of the division.

(1) The division [~~shall~~] may be a certification authority, and may issue, suspend, and revoke certificates in the manner prescribed for licensed certification authorities in Part 3 of this chapter.

(2) The division shall maintain a publicly accessible database containing a certification authority disclosure record for each licensed certification authority. [~~The~~] If the division operates as a certification authority, the division shall publish the contents of the database in at least one recognized repository.

(3) In accordance with Title 63, Chapter 46a, Utah Administrative Rulemaking Act, the division shall make rules as required by this chapter and in furtherance of its purposes, including rules:

(a) governing licensed certification authorities, their practice, and the termination of a certification authority's practice;

(b) determining an amount appropriate for a suitable guaranty, in light of:

(i) the burden a suitable guaranty places upon licensed certification authorities; and

(ii) the assurance of financial responsibility it provides to persons who rely on certificates issued by licensed certification authorities;

(c) for reviewing software for use in creating digital signatures and publish reports concerning software;

(d) specifying reasonable requirements for the form of certificates issued by licensed certification authorities, in accordance with generally accepted standards for digital signature certificates;

(e) specifying reasonable requirements for recordkeeping by licensed certification authorities;

(f) specifying reasonable requirements for the content, form, and sources of information in certification authority disclosure records, the updating and timeliness of such information, and other practices and policies relating to certification authority disclosure records; and

(g) specifying the form of certification practice statements.

Section 2. Section **46-3-202** is amended to read:

46-3-202. Performance audits and investigations.

(1) A certified public accountant having expertise in computer security, or an accredited computer security professional, shall audit the operations of each licensed certification authority at least once each year to evaluate compliance with this chapter. The division may specify qualifications for auditors in greater detail by rule.

(2) (a) Based on information gathered in the audit, the auditor shall categorize the licensed certification authority's compliance as one of the following:

(i) full compliance, which means the certification authority appears to conform to all applicable statutory and regulatory requirements;

(ii) substantial compliance, which means the certification authority generally appears to conform to all applicable statutory and regulatory requirements; however, one or more instances of noncompliance or inability to demonstrate compliance were found in the audited sample, but were likely to be inconsequential;

(iii) partial compliance, which means the certification authority appears to comply with some statutory and regulatory requirements, but was found not to have complied or not to be able to

demonstrate compliance with one or more important safeguards; or

(iv) noncompliance, which means the certification authority complies with few or none of the statutory and regulatory requirements, fails to keep adequate records to demonstrate compliance with more than a few requirements, or refused to submit to an audit.

(b) The auditor shall report the date of the audit of the licensed certification authority and resulting categorization to the division.

(c) The division shall publish in the certification authority disclosure record it maintains for the certification authority, the date of the audit, and the resulting categorization of the certification authority.

[~~(3) (a) The division may exempt a licensed certification authority from the requirements of Subsection (1) if:~~]

[~~(i) the certification authority to be exempted requests exemption in writing;~~]

[~~(ii) the most recent performance audit, if any, of the certification authority resulted in a finding of full or substantial compliance; and~~]

[~~(iii) the certification authority declares under oath or affirmation that one or more of the following is true with respect to the certification authority:~~]

[~~(A) the certification authority has issued fewer than six certificates during the past year and the total of the recommended reliance limits of all such certificates does not exceed $10,000;~~]

[~~(B) the aggregate lifetime of all certificates issued by the certification authority during the past year is less than 30 days and the total of the recommended reliance limits of all such certificates does not exceed $10,000; or~~]

[~~(C) the recommended reliance limits of all certificates outstanding and issued by the certification authority total less than $1,000.~~]

[~~(b) If the certification authority's declaration pursuant to Subsection (3)(a) falsely states a material fact, the certification authority shall have failed to comply with the performance audit requirement of this subsection.~~]

[~~(c) If a licensed certification authority is exempt under this subsection, the division shall publish in the certification authority disclosure record it maintains for the certification authority a~~

~~statement that the certification authority is exempt from the performance audit requirement.~~]