**KENYA BUREAU OF STANDARDS**

**ADOPTION PROPOSAL**

|  |  |  |
| --- | --- | --- |
| **Document Type:** | **Adoption proposal** | |
| **Dates:** | Circulation date | Closing date |
| 17/09/2018 | 17/10/2018 |
| **TC Secretary** | This form shall be filled, signed and returned to Kenya Bureau of Standards for the attention of **Allan Kimitei (kimiteia@kebs.org)** | |

The Kenya Bureau of Standards intends to adopt the International Standards as detailed here below .............................................................................................................................................

Number .  **ISO/TR14742:2010**

**Title** . *Financial services -- Recommendations on cryptographic algorithms and their use*

**Scope:**

This Technical Report provides a list of recommended cryptographic algorithms for use within applicable financial services standards. It also provides strategic guidance on key lengths and associated parameters and usage dates.

The focus is on algorithms rather than protocols, and protocols are in general not included in this Technical Report. However, in some cases, for example for some key agreement and some authentication protocols, there is no “underlying” algorithm, and in a sense it is the protocol that constitutes the algorithm. In this case, the mechanisms are included, in particular where they have security parameters that can be adjusted for higher or lower security.

Algorithmic vulnerabilities or cryptographic keys of inadequate lengths are less often the cause of security compromises in the financial industry than are inadequate key management or other procedural flaws, or mistakes in the implementation of cryptographic algorithms or the protocols that use them. However, compromises caused by algorithmic vulnerabilities are more systemic and harder to recover from than other kinds of compromises.

We are therefore seeking views from potential users in respect of the same. The Standard is available at the Kenya Bureau of Standards Information Centre. Please tick and fill your preference of the listed option. (If the spaces provided are not enough, please attach a separate sheet of paper).

Adoption acceptable as presented

...............................................................................................................................

...............................................................................................................................

Adoption proposal not acceptable because of the reason(s) below

...............................................................................................................................

...............................................................................................................................

Our Recommendations are as follows

...............................................................................................................................

...............................................................................................................................

Name and Signature (of respondent): ................................................

Position (of respondent): .....................................

On behalf of ......................................................................................... (Name of organization)

Date .........................................................................

**NOTE:** Absence of any reply or comments shall be deemed to be an acceptance of the proposal for adoption and **shall constitute an approval vote**.