

CEA Technical Report

Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1

CEA-TR-4

June 2014



CEA
Consumer Electronics Association

Documents
www.CE.org
Document Sharing Hub

NOTICE

Consumer Electronics Association (CEA®) Standards, Bulletins and other technical publications are designed to serve the public interest through eliminating misunderstandings between manufacturers and purchasers, facilitating interchangeability and improvement of products, and assisting the purchaser in selecting and obtaining with minimum delay the proper product for his particular need. Existence of such Standards, Bulletins and other technical publications shall not in any respect preclude any member or nonmember of CEA from manufacturing or selling products not conforming to such Standards, Bulletins or other technical publications, nor shall the existence of such Standards, Bulletins and other technical publications preclude their voluntary use by those other than CEA members, whether the standard is to be used either domestically or internationally.

Standards, Bulletins and other technical publications are adopted by CEA in accordance with the American National Standards Institute (ANSI) patent policy. By such action, CEA does not assume any liability to any patent owner, nor does it assume any obligation whatever to parties adopting the Standard, Bulletin or other technical publication.

This document does not purport to address all safety problems associated with its use or all applicable regulatory requirements. It is the responsibility of the user of this document to establish appropriate safety and health practices and to determine the applicability of regulatory limitations before its use.

This document is copyrighted by the Consumer Electronics Association (CEA®) and may not be reproduced, in whole or part, without written permission. Federal copyright law prohibits unauthorized reproduction of this document by any means. Organizations may obtain permission to reproduce a limited number of copies by entering into a license agreement. Requests to reproduce text, data, charts, figures or other material should be made to CEA.

(Formulated under the cognizance of the CEA **R7 Home Networks Committee.**)

Published by
©CONSUMER ELECTRONICS ASSOCIATION 2014
Technology & Standards Department
www.CE.org

All rights reserved

CEA Technical Report on Guidelines for Adding Strong Encryption and Authentication to Applications using ANSI/CEA-709.1

Contents

1. Purpose	1
2. References	1
3. Abbreviations	2
4. Scope	2
5. Requirements within the Scope	3
Secure Firmware Upgrade.	3
Identification and Verification.	3
Authentication/Non-Repudiation.....	3
Confidentiality.	3
Record/Playback Resistance.	3
Key Management.....	3
Key Protection.....	4
Revocation of Credentials.	4
Random Number Generation.	4
6. Architectural Decisions and Rationale.....	4

[This page intentionally left blank.]