In this paper, we propose a new Authenticated Lightweight Encryption algorithm coined ALE. The basic operation of ALE is the AES round transformation and the AES-128 key schedule. ALE is an online single-pass authenticated encryption algorithm that supports optional associated data. Its security relies on using nonces. We provide an optimized low-area implementation of ALE in ASIC hardware and demonstrate that its area is about 2.5 kGE which is almost two times smaller than that of the lightweight implementations for AES-OCB and ASC-1 using the same lightweight AES engine. At the same time, it is at least 2.5 times more performant than the alternatives in their smallest implementations by requiring only about 4 AES rounds to both encrypt and authenticate a 128-bit data block for longer messages. When using the AES-NI instructions, ALE outperforms AES-GCM, AES-CCM and ASC-1 by a considerable margin, providing a throughput of 1.19 cpb close that of AES-OCB, which is a patented scheme. Its area- and time-efficiency in hardware as well as high performance in high-speed parallel software make ALE a promising all-around AEAD primitive. © 2014 Springer-Verlag.