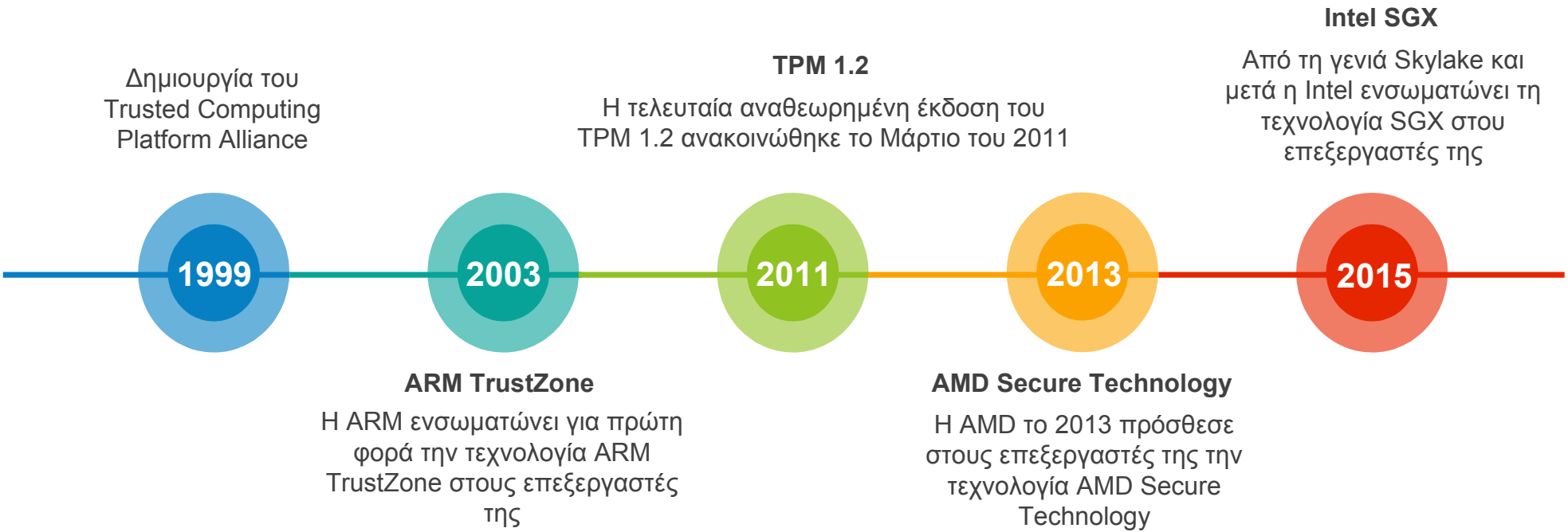
1999
Δημιουργία του Trusted Computing Platform Alliance
2003
ARM TrustZone
Η ARM ενσωματώνει για πρώτη φορά την τεχνολογία ARM TrustZone στους επεξεργαστές της
2011
TPM 1.2
Η τελευταία αναθεωρημένη έκδοση του TPM 1.2 ανακοινώθηκε το Μάρτιο του 2011
2013
AMD Secure Technology
Η AMD το 2013 πρόσθεσε στους επεξεργαστές της την τεχνολογία AMD Secure Technology
2015
Intel SGX
Από τη γενιά Skylake και μετά η Intel ενσωματώνει τη τεχνολογία SGX στου επεξεργαστές της