HDEF-ECDH 詳細評価 概要

HDEF は楕円曲線を用いた鍵配送法である．HDEF は使用する楕円曲線の trace を 3 に固定し，またその虚数乗法の判別式が小さい値になるように範囲を限定している．使用する楕円曲線の範囲を限定することは，相応の利点がない限り，受け入れることのできないことである．

HDEF の利点は，ユーザごとに異なる楕円曲線を使用できることと主張しているが，これが利点であるとは認め難く，逆にセキュリティホールを生みだす温床となりかねない．

以上から，HDEF は電子政府において使用する鍵配送法として適切でないと判断する．