

A UDX toolkit for IBM Z systems is tied to specific versions of the CCA code and the related host code. UDX is available for the Crypto Express6S (Secure IBM CCA coprocessor mode only) features. An UDX migration is no more disruptive than a normal Microcode Change Level (MCL) or ICSF release migration.

In z14 ZR1, up to four UDX files can be imported. These files can be imported from a DVD only. The UDX configuration window is updated to include a Reset to IBM Default button.

Consideration: CCA features a new code level starting with z13 systems, and the UDX clients require a new UDX.

On z14 ZR1, Crypto Express6S is delivered with CCA Level 6.0 firmware. A new set of cryptographic functions and callable services is provided by the IBM CCA LIC to enhance the functions that secure financial transactions and keys. The Crypto Express6S includes the following features:

- ▶ Greater than 16 domains support up to 40 LPARs on z14 ZR1
- ▶ Payment Card Industry (PCI) PIN Transaction Security (PTS) HSM Certification exclusive to CEX6S and z14
- ▶ Visa Format Preserving Encryption (VFPE) support, which was introduced with z13/z13s systems
- ▶ AES PIN support for the German banking industry
- ▶ PKA Translate UDX function into CCA
- ▶ Verb Algorithm Currency

Greater than 16 domains support

z14 ZR1 supports up to 40 LPARs. The IBM Z crypto architecture was designed to support 16 domains, which matched the LPAR maximum at the time. Before z13 systems, crypto workload separation can be complex in customer environments where the number of LPARs was larger than 16. These customers mapped a large set of LPARs to a small set of crypto domains.

Now in z14 systems, the IBM Z crypto architecture can support up to 256 domains in an adjunct processor (AP) with the AP extended addressing (APXA) facility that is installed. As such, the Crypto Express adapters are enhanced to handle 256 domains. The IBM Z firmware provides up to 85 domains for z14 Mxx and 40 domains for z14 ZR1 to customers (to match the current LPAR maximum). Customers can map individual LPARs to unique crypto domains or continue to share crypto domains across LPARs.

The following requirements must be met to support 40 domains:

- ▶ Hardware: z14 ZR1 and Crypto Express6S (or Crypto Express5S)
- ▶ Operating systems:
 - z/OS all functions require ICSF WD17 (HCR77C1), unless otherwise noted. WD17 supports z/OS V2R1, V2R2, and V2R3.
 - z/VM Version 6.4 with PTFs or newer for guest use.