



Adaptive Issuance Feature Enhancement Matrix

Adaptive Issuance includes multiple distinct software products. Each element of the suite serves to enhance the integration of Entrust issuance software and hardware, ultimately increasing flexibility and simplifying issuance complexities.

Adaptive Issuance software is regularly updated with enhancements and capabilities that provide security updates that protect your issuance environment and its customers.

This document outlines the updates made to components of our Adaptive Issuance suite that are fundamental to smart card and job management, highlighting some of the important changes that have improved security, performance, and functionality.



ENTRUST
SECURING A WORLD IN MOTION

Adaptive Issuance™ Chip Interface Software

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Capability to set up the APDU timeout, better supporting high network latency environments	•	•	•	•	•	•	•	•
Improved capability for automatic reconnection to the ObjectServer database	•	•	•	•	•	•	•	•
Capability for a data preparation or personalization script to reject cards when the Mastercard or Discover issuer certificate expires before the card expires	•	•	•	•	•	•	•	•
A new configuration utility replaces the former web browser-based configuration utility	•	•	•	•	•	•	•	•
For TLS 1.2 support, the SQL Server Native Client 11.0 driver is used for new ObjectServer databases	•	•	•	•	•	•	•	•
Custom names for "ADP" database		•	•	•	•	•	•	•
APS log scrubbing utility		•	•	•	•	•	•	•
MX9100 smart card licensing support		•	•	•	•	•	•	•
Open JDK		•	•	•	•	•	•	•
Translation from ISO-4 PIN block to ISO-1 and ISO-2			•	•	•	•	•	•
Installer and UI rebranding				•	•	•	•	•
Adaptive Issuance™ Production Analytics Solution - enhanced smart card statistics support				•	•	•	•	•
Remote ObjectServer database server support					•	•	•	•
ObjectServer database supports Windows authentication					•	•	•	•
ADP log configuration has changed, due to switching from log4j to logback							•	•
APS configuration files are now located in a directory identified by the AIS_APS_HOME environment variable. The default location is %ProgramData%\Datacard\Adaptive Issuance Suite\APS\.							•	•
ObjectServer database is now optional, and only required if using MULTOS Data Preparation and Personalization, Virtual 9000, or a smart card application that is dependent on general objects								•
Security updates	•	•	•	•	•	•	•	•

Adaptive Issuance™ EMV Data Prep and Perso

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Profile distribution supports naming each EMV server independently while also setting up server type as development, test, pre-production, or production (Enterprise edition)	•	•	•	•	•	•	•	•
Product Setup and BIN Setup state can be set to Working or Released (Enterprise edition)	•	•	•	•	•	•	•	•
For added security, EMV parameters are no longer editable with regard to a released setup (Enterprise edition)	•	•	•	•	•	•	•	•
From a central management location, profiles may be exported and shared among defined cross-environment or cross-site environments (Enterprise edition)	•	•	•	•	•	•	•	•
KMC Owner may be assigned from input data	•	•	•	•	•	•	•	•
BIN length may be edited in the data parsing setup screen	•	•	•	•	•	•	•	•
Software will default to production mode if the #CST# is not in the input data	•	•	•	•	•	•	•	•
Simulate mode parameter has been added in the UI	•	•	•	•	•	•	•	•
Support for new Mastercard BIN Range 2	•	•	•	•	•	•	•	•
Database password must be created also in Express and Plus editions	•	•	•	•	•	•	•	•
User management is enabled for all editions	•	•	•	•	•	•	•	•
Support for post-issuance set ups: Change PIN, reset locked-out PIN, deactivate a card, unlock applications	•	•	•	•	•	•	•	•
Editing of parameters in BIN setups (Express edition)	•	•	•	•	•	•	•	•
Extended APDUs up to 1984 Bits/chained APDUs are supported for personalization of larger certificates	•	•	•	•	•	•	•	•
PC/SC reader component can now be downloaded directly from the UI and is compliant with TLS 1.2	•	•	•	•	•	•	•	•
Standard M/Chip and DPAS data preparation setups reject cards if the issuer certificate expires before the card expires. Verification may also be applied to non-standard setups	•	•	•	•	•	•	•	•
Diagnostic Data Collector tool may gather EMV logs and configurations	•	•	•	•	•	•	•	•
Increase security for EMV Profile distribution by setting up a credential		•	•	•	•	•	•	•
Flexibility to set up cards that can expire on February 29 of leap years		•	•	•	•	•	•	•
BIN Attributes Setup to add static information (key version, owner, profile ID) based on the BIN from the input data		•	•	•	•	•	•	•
Job Alias allows to set alternate job ID option for runtime jobs		•	•	•	•	•	•	•
The card lock method at the end of the personalization can be configured through the EMV Profile Manager UI		•	•	•	•	•	•	•
Multiple data preparation profiles can be associated with a single product		•	•	•	•	•	•	•
Express and Plus editions support unrestricted import of profiles		•	•	•	•	•	•	•

Adaptive Issuance™ EMV Data Prep and Perso

continued

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Secure database connection is supported		•	•	•	•	•	•	•
Open JDK		•	•	•	•	•	•	•
BIN attribute visibility enhancements			•	•	•	•	•	•
Select all on EPM import			•	•	•	•	•	•
EPM import child profile impact summaries			•	•	•	•	•	•
Toggle on/off BIN attributes from the BIN management list			•	•	•	•	•	•
Import support of post-issuance profiles with TagValue elements			•	•	•	•	•	•
Manage ISO 3 and ISO 4 PIN block translation under control of the HSM			•	•	•	•	•	•
Support for managing KDC keys in perso profiles			•	•	•	•	•	•
Support for CARD keyword reading KDC key version from the chip			•	•	•	•	•	•
Profile export history via CSV			•	•	•	•	•	•
Advantis can be used in a data parsing setup			•	•	•	•	•	•
JCCB and VCCS data preparation options			•	•	•	•	•	•
Production Analytics Solution smart card statistics support				•	•	•	•	•
SCP03 authentication (3DES)				•	•	•	•	•
Key version/DKI selection based on card expiry				•	•	•	•	•
Delegated authentication (Express edition)				•	•	•	•	•
Installer and UI rebranding				•	•	•	•	•
Visa LOA checks based on final day of card expiry				•	•	•	•	•
Support for chained APDU modes 4, 5, and 6				•	•	•	•	•
Support for PRMISS key on DPS for Rupay qSparc dual interface profiles				•	•	•	•	•
Pre-personalization for NXP JCOP3 EMV P60				•	•	•	•	•
Support to Japan Debit						•	•	•
Support personalization of MULTOS CPS chips						•	•	•
EMV Profile Manager audit entries can be exported to a CSV file						•	•	•

Adaptive Issuance™ EMV Data Prep and Perso

continued

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Adds support for AES 256 keys for SCP03 (level 0 only)							•	•
Adds several new options for handling 8-digit BINs, including new input data items, BIN-level configuration settings, and new key owner configuration settings							•	•
BIN setups are now automatically ordered on change (import, creation, or edit of a BIN setup), and the manual controls for order BIN setups have been removed							•	•
EMV Profile Manager UI responsiveness is improved							•	•
Chip setups support specification of a custom APDU sequence for detecting the chip type							•	•
Profiles with a SuperTag list can be imported							•	•
Contactless indicator handling is improved							•	•
Adds support for including super tags in the SDA tag list							•	•
In first run configuration, the database configuration now defaults to use of the existing ADP database							•	•
The NXP delete command is supported							•	•
Adds card expiry date versus certificate expiry date check for CPA and PURE							•	•
Updates CPS data parsing to support Common Perso VNL "02.2" data format							•	•
EMV Profile Manager supports pasting a CPLC into a chip setup							•	•
Adds CPLC format Mode 2 for Perso Equipment ID							•	•
Updates CPLC data at the end of the perso so audit is the same value as the card							•	•
Adds large certificate support for Idemia EMV Pro and EMV Plus chips							•	•
Supports SCP03 cards using 128- and 256-bit KMCs, for levels 0, 1, and 3								•
Upon import of an EPM that will replace an existing EPM, a warning is displayed if the imported EPM has a new name								•
Allows nested super tags starting with FF to be resolved								•
Adds iCSC calculation for AMEX								•
Security updates	•	•	•	•	•	•	•	•

Adaptive Issuance™ MULTOS Data Prep and Perso

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Profiles selection based on MC4 and ML4 card formats	•	•	•	•	•	•	•	•
Run-time identification of the chip type for chip-specific data preparation and personalization via one-step mode	•	•	•	•	•	•	•	•
EMV records in MULTOS M/Chip ALUs reformatted to remove 0x00-byte padding before, between, and after TLVs in EMV records that were generated by the Adaptive Issuance M/Chip Advance for MICA-Compatible (MCAM) data generation application profile	•	•	•	•	•	•	•	•
The D-PAS, MCAM, MICA, and PURE R2 data preparation scripts ensure Application Expiration Date occurs after the Issuer Certificate Expiration Date	•	•	•	•	•	•	•	•
Chip reset is added before the Get Processing Options command to support newer chips	•	•	•	•	•	•	•	•
MULTOS MCA R3 v2.1 for MULTOS P18 cards.		•	•	•	•	•	•	•
MULTOS VSDC R5 v2.0 for MULTOS P18 cards		•	•	•	•	•	•	•
DPAS R3		•	•	•	•	•	•	•
ELO format Issuer Certificates in the Adaptive Issuance MULTOS PURE R2 application profile		•	•	•	•	•	•	•
PURE R2 - allow skipping the insertion of the iCVV value in the Track 1 data for ALU generation			•	•	•	•	•	•
Installer and UI rebranding				•	•	•	•	•
Ability to apply custom formatting to contactless Track2EquivalentData for VSDC R5							•	•
Additional capabilities to apply custom formatting to contactless track data for Visa and MC								•
Security updates	•	•	•	•	•	•	•	•

Adaptive Issuance™ Key Management

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
The keys now are stored encrypted in a database using a Device Master Key (DMK) stored in the HSM	•	•	•	•	•	•	•	•
There is no limit to the number of tokens (Enterprise edition)	•	•	•	•	•	•	•	•
There is no limit to the number of keys per token (Enterprise edition)	•	•	•	•	•	•	•	•
From a central management location, keys can be shared among defined cross-environment or cross-site environments (Enterprise edition)	•	•	•	•	•	•	•	•
An HSM pool is available to share HSM management, simplify the configuration, and prevent downtime (Enterprise edition)	•	•	•	•	•	•	•	•
User and security officer members may be assigned within groups	•	•	•	•	•	•	•	•
Groups may cross multiple HSM tokens	•	•	•	•	•	•	•	•
No maximum on number of user and security officers	•	•	•	•	•	•	•	•
User and security officers can change token PIN, which will be shared among defined tokens	•	•	•	•	•	•	•	•
New "HSM admin" role has been added	•	•	•	•	•	•	•	•
N of M may be modified after a token has been created	•	•	•	•	•	•	•	•
All token/key changes are automatically available to any registered HSM	•	•	•	•	•	•	•	•
HSM Firmware and certificate is bundled with Key Manager	•	•	•	•	•	•	•	•
Added HSM Maintenance Mode to perform maintenance tasks on the HSM without impacting production	•	•	•	•	•	•	•	•
HSM Client to HSM Server communication now uses standard HTTPS for communication	•	•	•	•	•	•	•	•
Applications can be authorized to log in to an HSM to access private keys in Read Only mode	•	•	•	•	•	•	•	•
Increased timeout for terminal entry of components from 180 seconds to 255 seconds	•	•	•	•	•	•	•	•
Following Adaptive Issuance Key Manager installation, all HSMs will go directly into maintenance mode. HSMs cannot be switched into production mode until the firmware has been updated	•	•	•	•	•	•	•	•
ProtectServer and Key Manager Firmware have been combined to simplify updates	•	•	•	•	•	•	•	•
HSM clock now synchronizes during HSM registration	•	•	•	•	•	•	•	•
Added the optional capability to set HSM PIN complexity rules when registering the HSM	•	•	•	•	•	•	•	•
KMS logs and configuration can now be gathered using the Diagnostic Data Collector tool	•	•	•	•	•	•	•	•
Encrypted database connection support	•	•	•	•	•	•	•	•
Open JDK	•	•	•	•	•	•	•	•

Adaptive Issuance™ Key Management

continued

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Translation from ISO-3 and ISO-4 PIN blocks to ISO-1, ISO-2, and ISO-3			•	•	•	•	•	•
TR-31 import			•	•	•	•	•	•
Import support of JCB key pairs, CA certificates, and issuer certificates			•	•	•	•	•	•
Delegated authentication (Plus edition)				•	•	•	•	•
Installer and UI rebranding				•	•	•	•	•
Optional HSM server client authentication				•	•	•	•	•
New nShield HSM/i configuration utility						•	•	•
nShield HSM/i can be used to import backup files created with versions prior to 6.4						•	•	•
nShield HSM/i Test and Development Kit can be installed on virtual machine						•	•	•
Audit entries can be exported to a CSV file						•	•	•
TR-31 export						•	•	•
New cryptographic API that can be used to integrate Adaptive Issuance Key Manager with other applications							•	•
HSM Client can be configured to dynamically select an HSM Server based on the token name							•	•
For Enterprise and Professional editions, cryptographic objects can now be replicated to secondary KMS databases without relying on SQL Server replication technology							•	•
TR-31 key block import/generation/entry now allows wrap/encrypt and unwrap/decrypt for keys with D0, K0, and P0 key usages							•	•
Adds cryptographic support needed for SCPO3 with AES 256							•	•
ProtectServer 1 HSMs can no longer be registered or updated.							•	•
Security World 12.80.4 is now the supported version								•
nShield firmware 12.72.1 is now the supported version								•
It is no longer necessary to tamper a ProtectServer HSM to update the SafeNet or Adaptive Issuance firmware, even if the corresponding certificate has expired								•
Security updates	•	•	•	•	•	•	•	•

HSMs

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
nShield HSM/		•	•	•	•	•	•	•
ProtectServer 2 PTK 5.8		•	•	•	•	•	•	•
ProtectServer 2 Firmware 5.03.01 and 5.03.02		•	•	•	•	•	•	•
ProtectServer 2 PTK 5.9			•	•	•	•	•	•
nShield HSM/ Test and Development Kit							•	•

Adaptive Issuance™ Job Enable & Data Access Software

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
A new configuration utility replaces the former web browser-based configuration utility	•	•	•	•	•	•	•	•
For TLS 1.2 support, the SQL Server Native Client 11.0 driver is used for new ObjectServer databases		•	•	•	•	•	•	•
Installer and UI rebranding				•	•	•	•	•
Security updates	•	•	•	•	•	•	•	•

Supported Platforms

Adaptive Issuance Version	6.5.1	6.6	6.7	6.7.1	8.2.2	8.2.3	8.2.4	8.2.6
Windows 10	•	•	•	•	•	•	•	•
Windows 11								•
Windows Server 2012 R2 and SQL Server 2012	•	•	•	•	•	•	•	
Windows Server 2016 and SQL Server 2016	•	•	•	•	•	•	•	•
Windows Server 2017 and SQL Server 2017	•	•	•	•	•	•	•	•
Windows Server 2019 and SQL Server 2019			•	•	•	•	•	•
Windows Server 2022								•
Microsoft Edge				•	•	•	•	•
Google Chrome					•	•	•	•

Learn more at [entrust.com](https://www.entrust.com)



Global Headquarters
 1187 Park Place, Minneapolis, MN 55379
 U.S. Toll-Free Phone: 888 690 2424
 International Phone: +1 952 933 1223