Definitive source for information

The SET protocol is described in Books 2 and 3. Because of the length of the documentation, it is possible that conflicts occur between the two books. In the event of conflicts, the following prioritized list should be used to determine which source is to be considered definitive (with items appearing first in the list being more definitive that items appearing later in the list):

Technical Bulletins published by SETCo
Book 3 Part II: ASN.1 Code
Book 3 Part I: Formal Protocol Definition
Book 2 Part I: System Design Considerations
Book 2 Part II: Certificate Management
Book 2 Part III: Payment System
Book 2 Appendices A, C, E, F, G, H, J, K, L, M, R
Book 2 Appendices T, U, V
Book 2 Appendices B, D, N, P, S

Reported problems with SET ASN.1

Line 164: missing definitions for hodMismatch.

Line 486: should contain optional LID-CA.

Line 567: should be formOrReferral

Line 665: invalid constraint, should be (0..50)

Line 1142: missing definition for invalidPI.

Line 1252: should contain TransIDs

Line 1290: missing definitions for originalProcessed, piMismatch, piAuthMismatch and authDataMismatch.

Line 1422: should contain BatchID.

Line 1838: TokenOpaque should be OPTIONAL.

Line 2007: implies that the OID should be rsaOAEPEncryptionSET when in fact it should be id-rsaEncryption. (Note: the "…" allows any OID to be used so there will be no decoding error when the correct OID is used.)

Line 2061: should be SubjectPublicKeyInfo {}.

Line 2731: should be IMPLICIT (Note: no impact on applications since SET does not used unauthenticated attributes.)

Line 3044: should be extensible to support additional attributes in SubjectAltName.

Line 3078: should have a constraint of (0..5)

Line 3096-3103: commenting out syntax statements violates ITU-T X.681.

Line 3164: should be SETString {}.

Line 3267: add EXPLICIT (Note: no change to bits on the wire.)

Line 3268: add EXPLICIT (Note: no change to bits on the wire.)

Line 3322: add EXPLICIT (Note: no change to bits on the wire.)

Line 3399: remove AdditionalPolicy

Reported problems with SET documentation

Book 2 Part I

Clarifications

Format of keys in SubjectKeyInfo

Language in SET messages is the same as RFC 1766 Content-Language.

Include processing steps for validating the BCI where appropriate.

More detail should be provided to explain the terminal and host capture models.

When a field is marked OPTIONAL in the ASN.1 that field may or may not appear in individual messages. Whether the field appears in a given instance of the message is described in the Formal Protocol Definition of Book 3 and the processing steps in the Certificate Management and Payment Systems portions of Book 2. Whether an application shall (or may) include support for the field is defined in Appendix E of Book 2.

Errors in text

Page 83 Step 3: should refer to the results of step 2.

Page 108 Step 1c: indicate that the ErrorOID should be for the first critical extension appearing in the message.

Page 108 Step 1d: indicate that the ErrorThumb should be for the certificate that appears lowest in the hierarchy. For example, if the cardholder certificate and the CCA certificate are inconsistent, the thumbprint of the cardholder certificate should be used.

Page 111: second *unknownXID* should be *unknownLID*.

Book 2 Part II

Clarifications

Define how to handle an expired CRL on the BCI. (I believe the appropriate action is to abort processing -TDL.)

All applications shall support the fourth root authentication method on page 132.

The software must be able to authenticate back to the earliest root certificate supported for a particular SET Version or to a root certificate that is in the trusted certificate cache.

A CA shall maintain a copy of all root certificates starting with the oldest certificate that was valid with the prior major release of the specification. A higher-level CA (root, brand, geo-political) shall send all these root certificates in any PKCS #7 response to a lower-level CA.

Describe the method for comparing BrandID fields in the certificate hierarchy with particular attention to the situation where the BrandID is in VisibleString format and the BrandID:Product is in Unicode format.

Clarify how to obtain a CA certificate for an key-exchange key with a request that is signed by a known signature key.

Clarify how payment gateway passes SETExtensions to PCA.

Specify OID to use in ContentInfo for SETQualifier.policyDigest.

Clarify that CertInqReq cannot be sent prior to receipt of CertRes.

All SET applications are required to fully validate certificates, certificate revocation lists and brand CRL identifiers prior to adding them to the application's trusted certificate cache.

An ErrorCode of invalidCertificate must be returned when a certificate's validity period is not within the validity period of the issuing CA.

The MerchantID sent in the certificate request messages is not necessarily the value that the CA will place in the MerchantData extension of the certificate.

Errors in text

Page 160 Step 5: Need three error codes.

Page 160 Step 7: should indicate that the Thumbs received match those sent in the ReqFormReq.

Page 171 Step 4: should indicate that an ErrorCode of wrapperMsgMismatch should be sent if the RRPID in the message does not match the value in the message wrapper and an ErrorCode of unknownRRPID should be sent if the RRPID does not match the one sent in Me-AqCInitReq.

Page 195 Step 2: should indicate that the Thumbs received match those sent in the CertReq.

Page 195 Step 3: should indicate that an ErrorCode of challengeMismatch should be sent if Chall-EE does not match and an ErrorCode of unknownLID should be sent if LID-EE does not match.

Page 197 Step 4.2: Refers to field that does not exist. Delete this step.

Page 208: The correct encoding of version is the value 2.

Page 241: Table 24 should distinguish the various CAs because they have different requirements.

Page 244: The correct encoding of version is the value 1.

Page 251: The correct encoding of version is the value 0.

Page 254: The additional policy attribute should not appear in a CA to CA certificate request.

Book 2 Part III

Clarifications

The merchant can have multiple acquirers for a single brand. It is the merchant's responsibility to establish the criteria to select the appropriate payment gateway certificate. Typically this will be a combination of the BrandID, BIN and promotional card name (which must be carried in an extension).

Any relationship between the cardholder's BIN and the merchant's BIN is coincidental.

The optional AcquirerBusinessID is assigned to the acquirer by the brand.

The BIN in PCertReq is the acquiring BIN.

Document procedure for maintaining the payment gateway's list of "used" payment instructions in light of authorization reversals (especially for recurring or installment payments).

If payment gateway creates batches, merchant learns BatchID from CapResPayload.

Payment gateway must transmit capture information to another system for clearing and settlement. (after processing steps on page 380 are performed)

Processing steps for BatchAdminReq must be changed to allow for BatchID being optional (when appropriate).

The CapPayload sent in a capture reversal, credit or credit reversal must be the same as that sent in the capture request. Note: the CapPayload sent in a capture request that follows a capture reversal is permitted to be (and most likely will be) different.

Clarify how to process multiple credits and credit reversals for a single transaction (particularly in light of there being no RRPID to link the credit to the capture item for split, recurring and installment payments).

Clarify the processing for multiple credits against the same transaction in a single batch.

Clarify how to process a credit for transaction processed as an authorization with CaptureNow.

The payment gateway will encrypt responses to the merchant using the key from most recently received merchant key-exchange certificate. A request message shall contain at most one merchant key-exchange certificate.

Clarify the impact of AuthReq with CaptureNow on open batches and appropriate error processing if there is a problem with the batch.

Clarify the processing step for reversing an authorization request with CaptureNow.

Clarify the impact of capture and credit reversals on batch totals.

If the number of authorizations exceeds InstallTotalTrans, return an AuthCode of recurringExpired.

Clarify the processing required for authorization referrals (callIssuer response).

PaySysID may be different for each authorization request performed.

CapTokens can be reused if after a capture reversal. (page 282 and payment gateway processing steps)

AuthReqData.mThumbs does not need to be retained for use in a future reversal request.

Errors in text

Page 300: Seconds are not optional for DER encoding of GeneralizedTime or UTCTime.

Page 313 Step 3.c: This step is incorrect and must be deleted.

Page 319 Step 2.f: BrandID is not optional in OIData.

Page 327 Step 3.A: Should return Error with ErrorCode of signatureRequired.

Page 328 Step 8: Does not specify action to take on failure.

Page 329 Step 1.f.4: Should indicate how software determines which merchant key to use to sign the message.

Page 355 Step 9: Should indicate that processing stops without performing the authorization.

Page 357 Step 2.b: captureNotSupported is a failure code; it does not indicate "successful" authorization.

Page 369 Steps 1 & 7: Refer to non-existent sub-fields of AuthRevTags. (should use AuthRevReqData.authReqData.authReqItem.authTags. transIDs)

Page 369 Step 5: says to send an Error message instead of a reply with an originalProcessed AuthCode.

Page 404 Step 2.b: Preamble could be clearer (some readers did not understand that the CapToken is optional).

Protocol problems

The BatchStatus does not include a BatchID so it is difficult (maybe impossible) to determine which batch is being referenced if multiple batches are covered by a single capture request/response.

There is no way to provide status for individual BINs in BatchStatus (in the event that multiple BINs are active for a single BrandID). This affects BrandBatchDetails, TransactionDetail, and ReturnTransactionDetail.

There is no way to identify the BatchSequenceNumber in capture reversals or credits.

Book 2 Appendices

Errors in text

Appendix E

Page 467: the bullets should be numbers to correspond to the conditions in the table that follows.

MessageIDs.localID-C is not optional for the cardholder and therefore the entire row should be deleted.

Appendix M

Delete rows for AuthToken, CapToken and CertReq in DigestedData table.

Appendix U and V

There are several errors in the sample encodings.

SET External Interface Guide

Clarifications

Content types for messages exchanged between CAs.

Content type for BCI Distribution message.

This document was last updated on August 23, 1999.