SETECS
Secure Transactions and Electronic Commerce Systems

Tel: (240) 535–2095 **http**://security.setecs.com **E-mail:** info@setecs.com

SETECS® OneCLOUD™
PIV Authentication and Authorization System

White Paper

Executive Summary

This document describes components, architecture, protocol and use of the SETECS® OneCLOUD™ Security System providing authentication and authorization services in a network and cloud environments. Authentication is based on three protocols: (a) local authentication using two factors – PIV card and user PIN, compliant with the FIPS 201 authentication standard, (b) remote authentication using PIV cards, certificates and strong authentication protocol, compliant with the FIPS 196 Strong Authentication standard, and (c) distributed authentication based on a single–sign on protocol, compliant with the SAML standard. Authorization is role–based, compliant to the XACML standard and supports three protocols: (a) policy administration protocol using Policy Administration Point (PAP), (b) policy decision protocol, performed by the Policy Decision Point (PDP), and (c) policy enforcement protocol for various Web applications, performed by the Policy Enforcement Point (PEP).

This document is created in compliance with the GSA PIV Authentication System Approval Procedure, v 2.0.0 and therefore can be used for certification of the product.

1. Introduction – Security Services

(1.1) SETECS® OneCLOUD™ Security System provides the following cloud security services to users and system administrators:

- *Local authentication* of users at their workstations using PIV cards. This service may be activated automatically during workstation boot process or manually, later, by users;
- *Remote authentication* based on FIPS–196 compliant challenge / response protocol using PIV cards that provide identification elements (PIV authentication certificate and CHUID) and for generate responses to the Server's challenges;
- *Single sign–on* protocol based on XACML/SAML standard and SAML Ticket. If SETECS® OneCARD™ PIV card is used, SAML Ticket is stored in the card, thus supporting user's mobility. With Government issued PIV cards, SAML Ticket is stored on the disk of user's workstation;
- *Key exchange* protocol based on PIV Key Exchange certificate stored in the card. The protocol is executed as the next step after completion of the strong authentication protocol and it establishes session key for communications between user's workstation and cloud servers. The same as with the SAML ticket – session key is stored either in the PIV card or on user's disk;
- *Role–based authorization* protocol controlling access to and actions with resources located in the cloud;
- *Confidentiality* (encryption) and *integrity* (hashing) of all messages exchanged between user workstation and cloud servers;
- *Encryption*, *digital signatures* and *enveloping* of documents shared in a group;
- Various *security management services*: registration of users in a cloud, management of roles and groups, administration of authorization policies, inspection of audit logs, etc.

2. System Components and Architecture

(2.1) SETECS® OneCLOUD™ Security System comprises several components, all shown in Figure 1 together with messages exchanged between them during strong authentication protocol, SSO protocol, and SAML ticket based authorization protocol.

(2.2) There are three types of components in each deployment environment:

- *User Workstations,* used by users to access network or cloud. SETECS® OneCLOUD™ Login client is installed at each workstation;
- *Central Security Server,* one instance in each environment;
- *Central Server Administration Station(s),* located in the deployment environment for remote administration of the components of the Central Security Server; and
- *Application (Web) Servers,* stand-alone located in the network and accessed directly or located in the cloud and accessed transparently.

(2.3) In Figure 1 various servers of the SETECS® OneCLOUD™ LACS and PACS are shown loaded in four separate hardware platforms:

- *Application Server* is the platform containing and running various cloud applications as cloud services (Three such applications are shown as example, A-1, A-2, and A-3). To enforce single sign–on and for enforcement of authorization policies, it is enhanced with the Policy Enforcement Pont (PEP);
- *Central Security Server* comprises four components: IDMS server, Strong Authentication server, Certificate Authority (CA) server, and XACML Policy Decision Point (PDP) server;
- *Security Administration Station* is used by Security Administrator(s) to manage all components of the Central Security Server;
- *User Workstation* has SETECS® OneCLOUD™ Login client, plus uses standard Internet Explorer browser to access Web applications.

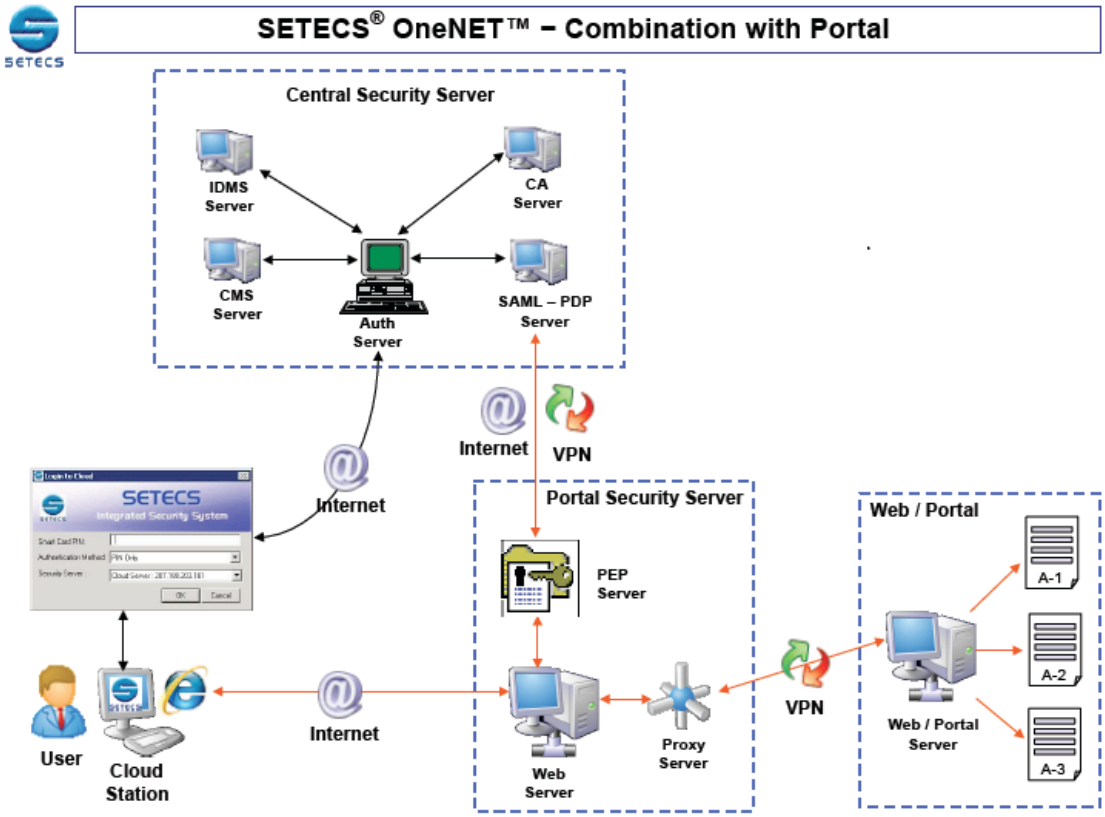

Figure 1: Components of the SETECS® OneCLOUD™ Security System

3. SETECS® Products

(3.1) SETECS® OneCLOUD™ Security System comprises the following products:

- SETECS® OneCARD™ PIV card – smart card, in possession of every user, containing fully loaded and personalized PIV applet;
- SETECS® OneCLOUD™ Login Client – client software installed at each user workstation;
- SETECS® OneCLOUD™ Single Sign-on Client – client software used at user workstations to access and read user PIV cards
- SETECS® OneNET™ Strong Authentication Server – the server performing strong authentication with the OneCLOUD™ Login module
- SETECS® OneNET™ Policy Decision Point (PDP) Server – the server issuing SAML ticket and making authentication and authorization decisions based on role–based authorization policy
- SETECS® OneNET™ Policy Enforcement Point (PEP) Server – the server using SAML ticket for enforcing authentication and authorization decisions made by the PDP server

(3.2) Supporting products are

- SETECS® OneMAN™ Identity Management (IDMS) Server – the server maintaining registration data for users, servers and all other system components
- SETECS® OnePKI™ Certificate Authority (CA) Server – the server supporting certificate management functions (issuing, distribution, verification and revocation of certificates)
- Physical Access Control (PACS) Server – the server enforcing physical access control decisions

4. Operations – PIV Authentication and Authorization

4.1 Asymmetric Challenge/Response Authentication using PIV Cards

(4.1) When users' registration data are either transferred or entered into the IDMS server's database and users have downloaded and installed at their workstations SETECS® OneCLOUD™ Login module, they may start accessing the network or cloud in a secure way. Every day, when starting their sessions with the network or the cloud, users must first activate OneCLOUD™ Login Client by double-clicking on its icon. The Client will display Login panel as shown in Figure 3 (a). The panel can be customized for individual agencies, shown in Figure 2 (b):

(a) Native Windows Login Panel (b) Customized Agency Login Panel

Figure 2: Cloud Client Login Panels

(4.2) User workstation must have smart cards reader with PINPad and each user must have PIV card. When login panel is displayed, user must insert his/her PIV card and give its PIN using reader's PINPad. The reader will access the card and submit the PIN for verification. If PIN is correct, the reader will activate the card.

(4.3) After successful local login, Cloud Login Client will read PIV authentication certificate from user's PIV card and submit it to the Strong Authentication server as the first message in the FIPS 196 strong authentication protocol. This action is labeled (1) in Figure 1. The Server will verify certificate using certificate chain validation and OCSP protocol and also user registration data in the IDMS server. If both verifications are successful, Strong Authentication server will execute FIPS-196 compliant challenge/response protocol with the Cloud Login Client. The Client will use PIV card to calculate responses to Server's challenges.

(4.4) The protocol is performed as the sequence of the following steps:

Step 1: User either clicks on an icon for Cloud Login module or starts browser and visits security–enhanced application server. In both cases, login panel, shown in Figure 2 is displayed.

Step 2: User inserts PIV card into the smart car reader and enters his/her PIN using smart card reader with the pin pad.

Step 3: If PIN is correct, smart card will be activated and PIV authentication certificate is read form the card.

Step 4: Certificate is sent to the OneNET™ Strong Authentication Server, representing the first, identification message in accordance with the FIPS 196 standard.

Step 5: Strong Authentication Server verifies user by verifying that
- User is registered in the IDMS and his/her status is correct
- Certificate is verified (against CRL and through verification of the certificate chain up to the top of the PKI)
- The status of the smart card is verified against the database of valid PIV cards, and
- User is verified to be registered in the PACS database.

Step 6: If all verifications in Step 5 complete successfully, Strong Authentication Server generates random number, envelopes it using user's public key (extracted from the user's certificate) and sends it back to the users as the challenge, in accordance with the FIPS 196 standard

Step 7: Challenge is passed into user's PIV card, where it is decrypted using user's private key stored in the card, creating user's response

Step 8: Response is returned to the Strong Authentication Server which verifies it against its original challenge

Step 9: If the verification is successful, Strong Authentication Server contacts OneNET™ Policy Decision Point (PDP) Server to issue SAML ticket to the user

Step 10: SAML ticket is issued for the user and returned to the Strong Authentication Server, which sends it back to the user

Step 11: User stores locally SAML ticket. If SETECS® OneCARD™ Card Management System was used to issue user's PIV card, SAML ticket is stored into user's PIV card. Otherwise, SAML ticket is stored into a local file. This step is labelled (2) in Figure 1.

(4.5) The final results of the authentication procedure is that

- User has SAML Ticket either in his/her smart card or on his/her disk,
- Security Server has the copy of the ticket issued to the user, and
- Shared secret session key is established between Cloud Login Server and user's workstation.

4.2 Single Sign–On Authentication Protocol using SAML Ticket

(4.6) When a user wants to access cloud and use its services provided by its applications, he/she will activate the browser and direct it to the network's or cloud's Web application server (URL). Web Applications server will display Network/Cloud Home page. This step is

labeled (3) in Figure 1. With security extensions (PEP Server) installed at the Web Application Server, Policy Enforcement Point (PEM) server will intercept user's access request. It will send another components of the Cloud Login Client to the user's workstation and fetch SAML Ticket from user's smart card. It will send SAML Ticket back to the PEP Server. This step is labeled (3) in Figure 1.

(4.7) PEP server will pass SAML ticket to the PDP Server (step (4) in Figure 1), which will recognize it and confirm it as the valid ticket recently issued to the user. PDP will return its decision back to the PEP (step (5) in Figure 1), which will return the decision back to the user (step (6) in Figure 1). This confirmation represents single sign–on into the network or cloud. The ticket has (default) life–time of eight hours.

4.3 Authorization Protocol using FASC–N

(4.8) During issuing of PIV Card, SETECS OneCARD (PIV) Card Management System, for each user will create FASC–N as the combination of 14 digits: agency code (4 digits), system code (4 digits), and credential (card) number (6 digits). These three attributes will be entered into the user's database entry in the IDMS (OneMAN™ Database table.

(4.9) When users are entered in the authorization (XACML) policy groups, all three attributes of their FASC–N and their Personal Identifier (PI) are also entered in the Policy. This step is shown in Figure 3:

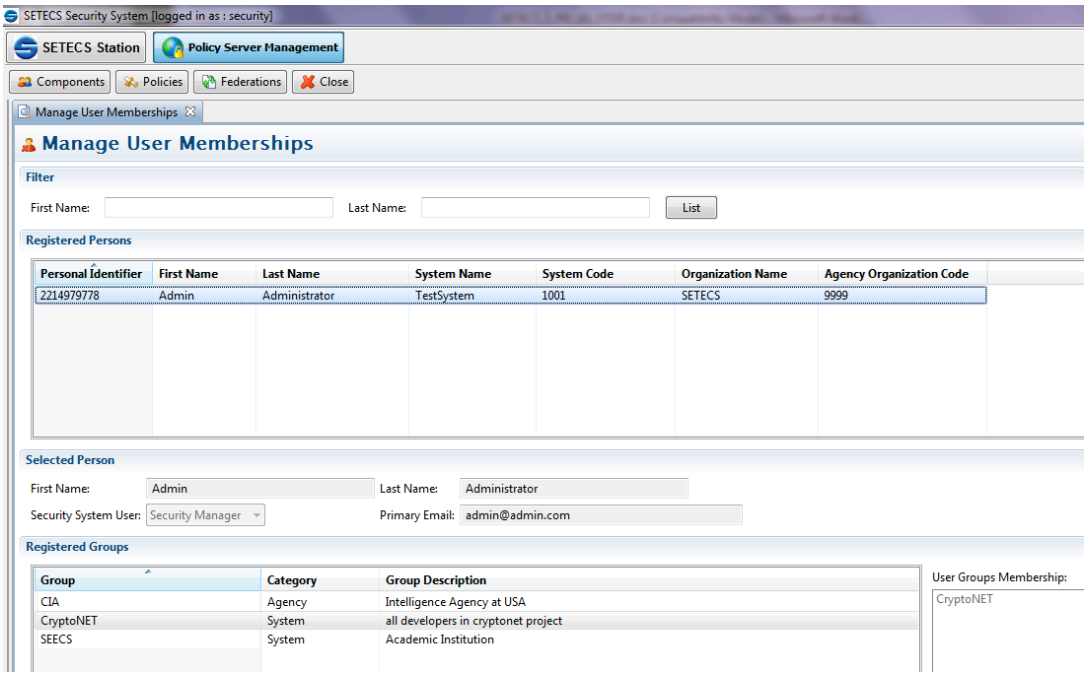

Figure 3: Registration of Users and Their FASC–N in Authorization Policy

(4.10) After requests are received submitted by users, PEP server will pass authorization requests to the PDP server for approval. The request contains user ID, action required, and indication of all network/cloud resources needed to fulfill the request. User ID comprises FASC–N and PI, so authorization decisions are made based on FASC–N. PDP Server will, using XACML policy, make the decision to approve or deny the request. If approved, home page of the requested application will be displayed to the user.

5. Compliance to the PIV Authentication Procedure

This section lists requirements in the GSA document PIV Authentication System Approval Procedure, v 2.0.0 and explains how SETECS® OneCLOUD™ Security System meets all these requirements. Complementary document is Vendor Test Data Report.

PIV Authentication System Approval Procedure, v 2.0.0 has the following requirements for PIV Authentication system product:

5.1 PIV-AS.1: Smart Card Reader with PINPad

PIV–AS.1	Reader used shall be listed on FIPS 201 Evaluation Program Approved Products List under the Transparent Reader category.

Compliance: SETECS® is using smart card reader produced by HID Global (formerly OmniKey), model CardMan 3621 Contact Smartcard Pin Pad Reader. The reader has pin pad and it is listed in the GSA APL as item number 84.

Approval Mechanism: Inspection of the GSA APL (http://fips201ep.cio.gov/apl.php)

5.2 PIV-AS.2: Asymmetric Challenge/Response Protocol with PIV Card

PIV–AS.2	The Product shall be capable of performing an asymmetric cryptographic challenge/response with the PIV Card.

Compliance: The product supports an asymmetric challenge/response protocol using PIV card, based on the FIPS 196 standard

Approval Mechanism: Test 1 in the Vendor Test Data Report

5.3 PIV-AS.3: Asymmetric Algorithms

PIV–AS.3	The PACS must support all of the asymmetric algorithms permitted for the PIV Authentication Key, as specified in Table 3-1 of SP800-78-3.

Compliance: Table 3-1 from the SP800-78-3 standard is reproduced below. For PIV authentication, RSA algorithm is required with key size 1024 or 2048. SETECS® PIV Authentication System uses RSA algorithm with 1024 bits key size.

Approval Mechanism: Inspection of SETECS® Security Policy (Appendix) and Test 2 in the Vendor Test Data Report

Table 3-1. Algorithm and Key Size Requirements for PIV Key Types

PIV Key Type	Time Period for Use	Algorithms and Key Sizes
PIV Authentication Key	Through 12/31/2013	RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	RSA (2048 bits) ECDSA (Curve P-256)
Card Authentication Key	Through 12/31/2010	2TDEA 3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	1/1/2011 through 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature Key	After 12/31/2008	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
Key Management Key	After 12/31/2008	RSA key transport (2048 bits); ECDH (Curves P-256 or P-384)

5.4 PIV-AS.4: PIN

PIV–AS.4	The reader shall be able to provide the personal identification number (PIN) to the card to access the PIV Authentication Key stored on the PIV Card.

Compliance: SETECS® is using OmniKey CardMan smart card reader model 3821 with the PIN pad. The reader is certified by the GSA and it is on the GSA APL (item number 85)

Approval Mechanism: Inspection of the GSA APL (http://fips201ep.cio.gov/apl.php) and Cloud Login Client audit log (Test 3)

5.5 PIV-AS.5: Smart Card Reader with Integrated PIN Input Device

PIV–AS.5	Reader used shall include integrated PIN input device.

Compliance: SETECS® is using OmniKey CardMan smart card reader model 3821 with the PIN pad. The reader is certified by the GSA and it is on the GSA APL (item number 85). The reader has integrated PIN input device

Approval Mechanism: Reader documentation available at http://www.hidglobal.com/prod_detail.php?prod_id=190

5.6 PIV-AS.6: Signature and path Validation

PIV–AS.6	The response signature is verified and standards-compliant (IETF X.509 path validation) PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.

Compliance: SETECS® OneNET™ Strong Authentication server verifies signature of the response, created by the card using PIV Authentication certificate, whose validity is verified by (a) verifying signatures of all certificates up to the top of the PKI, (b) verifying that the self–signed certificate is in the Trusted list, and (c) verifying the revocation status of the certificate PIV Authentication certificate

Approval Mechanism: Validation of the Strong Authentication server audit log (Test 4)

5.7 PIV-AS.7: FASC-N for Access Control Decisions

PIV–AS.7	All access control decisions are made by comparing the 14 decimal digits FASC-N Identifier, and optionally the values of additional FASC-N fields, against the ACL entries.

Compliance: SETECS® OneNET™ Policy Decision Point (PDP) server creates access control decisions based on the 14 digits FASC-N number. Optionally, Personal Identifier (PI) may also be included in the Authorization Policy (XACML).

Approval Mechanism: Validation of the Policy Decision Point server audit log (Test 5)

5.8 PIV-AS.8: Cryptographic Modules

PIV–AS.8	The cryptographic module(s) used shall be validated to FIPS 140-2.

Compliance: Cryptographic modules on the client side are performed by the PIV card. SETECS® PIV Authentication system uses only smart cards approved by GSA and on the PIV APL list, where FIPS 140–2 compliance is the prerequisite. In particular, for this certification SETECS® is using Gemalto PIV card (item number 378).

On the Server side, SETECS® uses OpenSSL crypto library, which is certified by NIST and appears on the list of FIPS 140–2 certified products

Approval Mechanism: Inspection of the GSA APL (http://fips201ep.cio.gov/apl.php) and NIST FIPS 140–2 certification list (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm) (item number 1111)

5.9 PIV-AS.9: PIV Middleware

PIV–AS.9	If the Product uses middleware to communicate with the PIV Card (e.g. as part of Card Management System functionality), this middleware is approved by the GSA FIPS 201 Evaluation program as approved PIV Middleware.

Compliance: PIV Authentication system does not uses PIV middleware, but SETECS PIV middleware is approved by GSA and appears on the APL (item number 40).

Approval Mechanism: N/A

5.10 PIV-AS.10: SCSP

PIV–AS.10	If the Product interfaces with a Certificate Validator to perform certificate path discovery and validation, it uses a GSA FIPS 201 EP approved SCVP client.

Compliance: PIV Authentication system does not use SCVP Client

Approval Mechanism: N/A

Appendix: Security Policy

```
# ------------------------------------------------------------------
# Security Policy file contains parameters for the Authentication Server
# ------------------------------------------------------------------

[DEFAULT]
EntityType                    = Server # [TCA,PolicyCA,HCA,LCA,SCA,User,Server,PDP]
AltName                       = Local CA Server,Networking Division,SETECS Inc.,US
                              # Must be given, if AltName PKIX ext selected
KeyAlgorithm                  = RSA # [RSA, DSA]
KeyLength                     = 1024 # [512, 768, 1024, 2048]
CertificateValidPeriod        = 365 # [any number of days]
PrivateKeyUsagePeriod         = 9990 # [any number of days]
CRLUpdateInterval             = 30 # [any number of days - one month
recommended]
CRLHashAlgorithm              = SHA1 # [SHA1, MD2, MD5]
CertRequestHashAlgorithm      = SHA1 # [SHA1, MD2, MD5]
CertificateHashAlgorithm      = SHA1 # [SHA1, MD2, MD5]
PublicKeyHashAlgorithm        = SHA1 # [SHA1, MD2, MD5]
TunnelingAlgorithm            = DES-CBC # [DES-CBC, DES-CDMF] Must be given to
create Tunneling SET extension
NameConstraintsPermitted      = CA,Unit,SETECS,US,-#
NameConstraintsExcluded       = CA,Unit,Company,US,-#
AuthorityInfoAccessLocation1  = caIssuers;URI:http://192.168.0.2/
AuthorityInfoAccessLocation2  = caIssuers;URI:http://192.168.0.2/
AuthorityInfoAccessLocation3  = http://192.168.0.2/
CRLDistributionPoint          = -,-,-,-,ldap://128.164.82.52:389

# ------------------------------------------------------------------
# This section describes PKIX extensions, as described in Book 2, p 241.
# By default KeyUsage extension is automatically set,
# but for the completeness all extensions are defined.
# Set values to '1/0' in order to create/remove extensions.
# ------------------------------------------------------------------

[PKIX_EXTENSIONS]
AuthorityKeyIdentifier        = 1 # [1/0] -- not critical, not relevant for
the TCA
KeyUsage                      = 1 # [1/0] -- critical
PrivateKeyUsagePeriod         = 0 # [1/0] -- not critical, but required by SET
CertificatePolicies           = 1 # [1/0] -- critical
PolicyMappings                = 0 # [1/0] -- not critical
NameConstraints               = 1 # [1/0] -- critical
AuthorityInformationAccess    = 0 # [1/0] -- not critical
CRLDistributionPoint          = 1 # [1/0] -- not critical
# If the following two AltName extensions are set to 1,
# you must give the AltName in the [DEFAULT] section
SubjectAltName                = 1 # [1/0] -- not critical
IssuerAltName                 = 1 # [1/0] -- not critical
BasicConstraints              = 1 # [1/0] -- critical
ExtendedKeyUsage              = 1 # [1/0] -- 0:NO 1:Yes not critical 2:Yes and
critical

[PIV_EXTENSIONS]
PIVinterim                     = 2 # [1/0] -- 0:NO  1:Yes (Value is False)
2:Yes (Value is True)


# ------------------------------------------------------------------
# This section describes PKIX CRL extensions
# ------------------------------------------------------------------
[CRL_EXTENSIONS]
AuthorityKeyIdentifier        = 0 # [1/0] -- not critical
CRLNumber                     = 1 # [1/0] -- not critical, but needed for SET
to create BCI
```

```
# ---------------------------------------------------------------------
# This section describes SET private extentions
# By default all SET extensions are skipped,
# So you must set each of these extensions if you need it.
# Set values to '1/0' in order to create/remove extensions.
# ---------------------------------------------------------------------

[SET_EXTENSIONS]
HashedRootKey                = 0 # [1/0] -- critical
CertificateType              = 0 # [1/0] -- critical

# The following four extentions are not critical
MerchantData                 = 0 # [1/0] -- Not relevant for CAs, so set to '0'
CardCertRequired             = 0 # [1/0] -- Not relevant for CAs, so set to '0'
Tunneling                    = 0 # [1/0] -- Not relevant for CAs, so set to '0'
SetExtensions                = 0 # [1/0] -- Whether SETExtention is specified

# ---------------------------------------------------------------------
# This section describes Merchant information
# If you set the merchantData extension, then this section must be filled.
# ---------------------------------------------------------------------

[MERCHANT]
MerAuthFlag                  = - # Not relevant for CAs
MerID                        = - # Not relevant for CAs
MerAcquirerBIN               = - # Not relevant for CAs
MerLanguage                  = - # Not relevant for CAs
MerName                      = - # Not relevant for CAs
MerCity                      = - # Not relevant for CAs
MerStateProvince             = - # Not relevant for CAs
MerPostalCode                = - # Not relevant for CAs
MerCountryName               = - # Not relevant for CAs

# ---------------------------------------------------------------------
# This section describes Policy information
# If you set the CertificatePolicies extension, this section must be filled.
# ---------------------------------------------------------------------

[POLICY]
PolicyOIDs                   = 2.16.840.1.101.3.1.48.1,2.16.840.1.101.2.1.12.1.1
PolicyMappings               = 2.16.840.1.101.3.1.48.1,2.16.840.1.101.2.1.12.1.1
PolicyQualifierID            = PKIPolicy # [TestPolicy, SETPolicy]
PolicyURLs                   = http://www.setecs.com/CertPolicy.htm
# Cert Policy HTML file
PolicyDigest                 = - # The digest of the Cert Policy HTML file
AdditionalPolicyURL          = - # Additional Cert Policy
PolicyEmail                  = - # E-mail of the Policy admin
TerseStatement               = - # "Here comes description of cert usage"

# ---------------------------------------------------------------------
# This section describes ExtendedKeyUsage information
# If you set the ExtendedKeyUsage extension, this section must be filled.
# ---------------------------------------------------------------------
[EXKEYUSE]
exKeyUsage                   = 2.16.840.1.101.3.6.7
```