Certicom Device CA for ZigBee Smart Energy

Order Fulfillment Process

Customer Guide

May 2010

5520 Explorer Drive, 4th Floor, Mississauga, Ontario, Canada, L4W 5L1

main 905-507-4220 • support 1-800-511-8011 • fax 905-507-4230

Certicom ECQV Device Certificates for ZigBee Smart Energy Devices

The Certicom Device CA for ZigBee Smart Energy provides a common root of trust for ZigBee Smart Energy Profile devices, enabling out of the box interoperability and security, lowering the total cost of ownership for utilities and metering companies while enhancing the security and integrity of the utility network devices with a bandwidth efficient public key infrastructure (PKI).

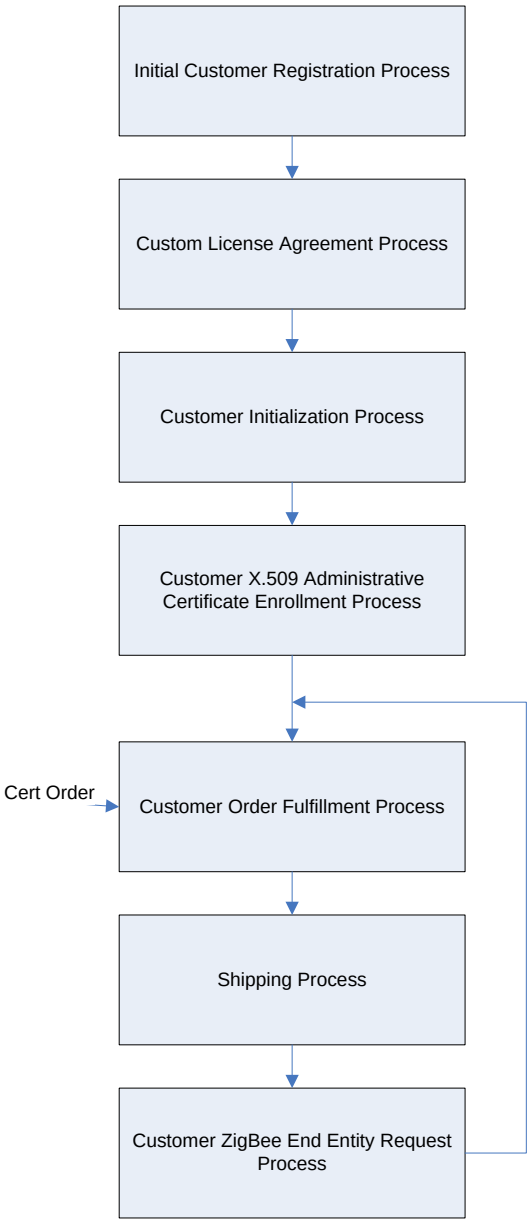
The Certicom ZigBee Smart Energy PKI service issues Elliptic Curve Qu Vanstone (ECQV) *implicit* certificates to eligible subscribers - ZigBee Alliance members with ZigBee Smart Energy Profile Certified devices.

ECQV device certificates bind manufacturer information and device MAC addresses to ECC public key pairs. Certificates are used to secure a ZigBee Smart Energy device as it gets enrolled on the network using an authenticated key agreement scheme, and further to sign a device's Smart Energy Profile messages.

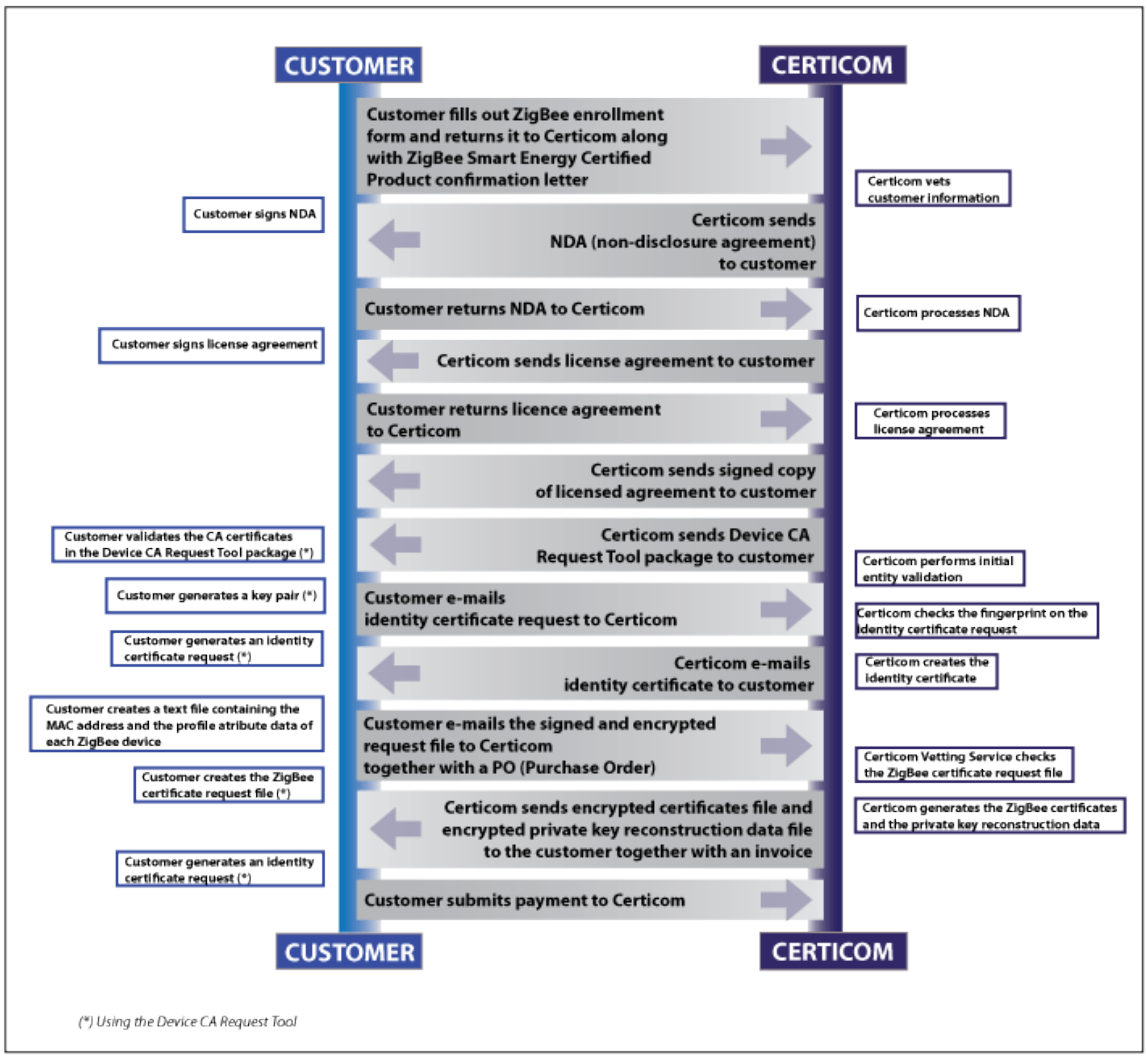
Certicom Device Certification Authority for ZigBee Smart Energy

ZigBee Alliance member companies manufacturing ZigBee Smart Energy Certified products can register for production certificates from the Certicom *Device CA ZigBee Smart Energy subscriber enrollment* webpage www.certicom.com/index.php/regzigbee. This Guide explains the requirements, process and processing timeframes at a high level.

High Level ZigBee Order Fulfillment Processes



A number of interactions between Certicom, the customer and potentially the ZigBee Alliance are required to determine eligibility, gather enrollment information, execute a subscriber agreement and issue certificates. The information and process flow is depicted below. Timeliness of the entire process from enrollment to device certificate issuance depends upon the completeness and accuracy of the initial application, the availability of subscriber documentation from the ZigBee Alliance, corporate charter documents and the complexity of the subscriber's corporate structure. Preparing and executing the NDA and subscriber agreement will require a minimum of 10 business days, more typically 15, and could take significantly longer for more complex license requests. Each certificate issuance step (administrative and device certificate order) will require up to 5 days.



Step 1. Initial Customer Registration Process

ZigBee Smart Energy device certificates are issued only to manufacturers whose ZigBee Smart Energy Profile products are certified by the ZigBee Alliance. Once a manufacturer has a ZigBee Smart Energy Profile certified product they can enroll in the ZigBee Smart Energy PKI. This requires executing the Certicom ZigBee Smart Energy Profile subscriber agreement and paying the appropriate fees. This process begins with registration.

The registration webpage located at www.certicom.com/index.php/regzigbee will prompt the Applicant to complete an online form. Detailed information such as ZigBee Alliance Manufacturing Code, ZigBee Smart Energy Certification ID #, Primary Contact, Technical Contact, Billing Contact and Signatory Information will be requested. Providing accurate information in the initial request will speed the contracting process.

On submission the enrollment form is automatically emailed to Certicom. A Certicom Device CA representative will screen the request and contact the Primary Contact to accept or reject the request based on the information supplied and records from the ZigBee Alliance. This process should be completed typically within two business days. . The Certicom ZigBee Processing Coordinator (ZPC@Certicom.com) may contact the customer's Primary Contact to confirm enrollment information.

Note:

To be eligible for enrollment the Applicant's company must have a ZigBee Alliance assigned Manufacturing Code - if they do not have a Manufacturing code the ZigBee Alliance can supply one. This is required to qualify an Applicant.

The ZigBee Alliance sets baseline subscriber eligibility requirements by setting ZigBee Smart Energy certification requirements using external test houses. To reduce the delay between certification and certificate issuance Certicom will accept Applications with a test house certification pending. Device Certificates will not be issued until Certification is confirmed by the ZigBee Alliance, typically via a Certification Confirmation Letter.

Step 2. NDA and Subscriber License Agreements

Within 2 to 3 days of an Applicant qualification, a Certicom representative will follow up to provide service timelines and pricing information and discuss the needs of the enrolling organization with respect to ZigBee Smart Energy certificates such as whether multiple affiliates will need to be enrolled and what operating environment (Linux or Windows) will be used when ordering certificates.

At this point Certicom will need to confirm signatory and registered legal address details and collect corporate charter documents in order to prepare legal agreements. A new customer will be required to first sign a Certicom Non-Disclosure Agreement (NDA) and then a Subscriber License Agreement. Both agreements are mandatory for a customer to enroll in the Certicom ZigBee Smart Energy device certificate service.

NDA

In order to facilitate the completion of the NDA process, Applicants will be asked to provide a Certificate of Incorporation for their company, the registered corporate address as well as the name and role of the person signing the NDA. A standard Certicom NDA with no redlines can typically be processed in less than 5 business days after all documentation has been provided.

Some NDAs require special processing if for example a company has a complex corporate structure, as is common with affiliates of multi-national companies. In such instances we anticipate this additional requirement will result in significant delay and in such cases an applicant will be asked to provide the Certificate of Incorporation and registered company address for each subsidiary and affiliate who will be purchasing ZigBee Smart Energy Device Certificates for their Certified Products.

Non-Certicom NDAs will not be accepted.

Subscriber Agreement

The NDA is followed up with a subscriber agreement which authorizes the purchase of ZigBee Smart Energy certificates and sets terms and conditions on their use. This is prepared only after an NDA has been completed. Financial statements may be required for credit approval.

In order to prepare the license the customer must indicate whether they are choosing the low unit cost annual subscription service or the no annual fee á la carte service option.

Pricing information for á la carte or subscription information is available in the ZigBee Frequently Asked Questions (FAQ) on Certicom's website.

Once the Applicant has signed and returned the subscriber agreement an additional 5 to 10 business days are required to complete the signature loop.

Step 3. X.509 Administrative Certificate Request Process

In order to request and receive ZigBee device certificates, customers require an X.509 Administrative Certificate issued by Certicom to authorize subsequent device certificate orders and to decrypt shipments from Certicom.

The Administrative Certificate request is created using a Certicom certificate request tool (CA Reqtool). This command line utility creates Administrative and bulk ZigBee device certificate requests and performs pre and post processing on bulk requests. A User Guide details each step in the technical process. The CA Reqtool utility is available for both Windows and Linux operating environments.

The customer's Primary Contact will be shipped the CA Reqtool when the subscriber agreement is signed by both parties.

Customers will first use the CA Reqtool to create a PKCS #10 formatted Administrative Certificate request and email the request to ZigBeeOrders@certicom.com. The ZigBee Administrator, upon receipt of the request, will contact the Primary or Technical Contact to perform an out-of-band authentication procedure called a Fingerprint. This procedure is performed to confirm that the PKCS #10 certificate request has in fact been sent by an authorized contact representing the enrolled organization. It is imperative that a Primary or Technical Contact can be reached by phone in order to validate inbound Administrative Certificate orders or respond to any Certicom queries.

A purchase order is required at this stage for companies enrolling under the subscription model. It may include line items for a subsequent bulk certificate request and administrative processing fee.

Once the ZigBee Administrator has a valid certificate request, it will be forwarded to the Certicom Device CA Operations for Order Fulfillment. Valid orders are typically turned around in 5 business days provided that a purchase order has been approved. A customer with an X.509 Administrative Certificate is now able to request ZigBee device certificates.

Step 4. Bulk ZigBee Device Certificate Request Process

ZigBee device certificates are requested by the customer using the CA Reqtool. The process is similar to the X.509 certificate request, however the CA Reqtool requires a valid Administrative Certificate in order to create the order.

The customer will create a bulk certificate request using the CA Reqtool and email it to ZigBeeOrders@certicom.com along with the required purchase order if one has not already been sent. Smaller requests may be emailed, while larger requests can be uploaded through a Certicom web interface (email ZigBeeOrders@certicom.com for the upload link instructions).

Once subscriber eligibility has been confirmed with the ZigBee Alliance, and provided that it has not subsequently been revoked, and the PO has been accepted by Certicom, Certicom will begin the device certificate vetting and issuance process.

Certicom will verify each order is correct and matches the Purchase Order. If a PO has not been received or there is a mismatch, Certicom will notify the customer of the error and request a correction to the request and/or a new Purchase Order that matches the request and the customer license agreement (and the corresponding subscriber or á la carte fees).

In terms of technical verification, the ZigBee Administrator will vet the request for correctness, ensuring the digital signature authorizes the request, that there are no duplications in MAC addresses from any previous orders, and that the customer is authorized to specify the designated ZigBee Manufacturing Code in each device certificate requested. If the vetting fails the ZigBee Administrator will contact the requestor and ask for a new certificate request to be generated.

Once the ZigBee Administrator has a bulk certificate request, it will be forwarded to the Certicom Device CA Operations for Vetting and Order Fulfillment. Vetting errors will be rejected with a notification within 2 business days. Valid orders will be processed and are typically turned around in 5 business days provided that a purchase order has been approved.

Once issued certificates will be delivered and the order invoiced. For companies with a good credit history, certificates can be issued and shipped based on a purchase order; otherwise delivery of certificates may require payment in advance.

.