ECDSA Signing Steps in Detail:

(see e.g. Paar, Pelzl, "Understanding Cryptography", Springer Heidelberg 2010, ISBN 978-3-642-04100-6)

1. Chose a secret ephemeral key k_e
(Use a secure and properly initialized Pseudo Random Number Generator to generate an Integer k_e smaller than, but of same bytelength as domain group order q.

2. Calculate k_e^{-1} using the Chinese Remainder Theorem.

3. Calculate point $R = k_e \cdot A$
(A is the domains primitive point generating the group.)

4. Select x-component of Point R and denote it as "r".

5. Compute hash value $hash$ of file to be signed.

6. Provide secret private key d

7. Calculate $s = \left(\left(hash + d \cdot r \right) \cdot k_e^{-1} \right) mod\, q$

8. Create signature file containing a ***domain identifier*** with ***hash specifier*** for information and the signature components r and s.

ECDSA Signature Verification Steps in Detail:

1. Retrieve signers public Key B from a trusted source and r , s from signature file.

2. Retrieve parameters of domain used by signer (got domain id from signature file).

3. Calculate auxiliary value $w = s^{-1} mod\, q$.

4. Calculate auxiliary value $u1 = \left(w \cdot hash \right) mod\, q$.(Hash algorithm specified in signature file.)

5. Calculate auxiliary value $u2 = \left(w \cdot r \right) mod\, q$.

6. Compute point $P = {}_{u1} \cdot A + {}_{u2} \cdot B$.

7. Accept signature if x-component of P equals r : $\overset{?}{\left(x_P \equiv r \right)} mod\, q$, reject otherwise.