Purpose
To establish a policy governing the treatment of electronic signatures by the Utah Department of Transportation (Department) in accordance with the Uniform Electronic Transactions Act (UETA).

Policy
A signature will not be denied legal effect or enforceability solely because it is electronic. The Department will recognize the validity of an electronic signature unless specifically prohibited or restricted by law, rule, or policy.

The Department will specify in this policy any exceptions to or restrictions on its acceptance of a handwritten signature, electronic signature, digital signature, or digital certificate.

Electronic signatures encompass any sound, symbol, or process that conveys a person’s intent to sign a record. Electronic signatures indicate consent, but do not provide any assurance regarding the identity of the signer or the veracity of the signature. Digital signatures are a subset of electronic signatures, and offer some type of mechanism to verify the identity of the signer. Digital certificates are digital signatures that use Public Key Infrastructure (PKI) technology to guarantee the identity of the signer.

The Department will not accept electronic signatures that are not digital signatures for:
- Contracts and agreements with vendors and other government agencies;
- Documents requiring a signature relating to employment, terms of employment, and employment actions; or
- Documents requiring a signature relating to employee time reporting, leave balances, and payroll actions.

The Department will accept only digital signatures, unless an exception is granted by the Standards and Design Engineer or designee, for:
- Standard Drawings;
- Design Exceptions, Design Waivers, and Deviations from Department Standards; or
- Plan Sheets.
<table>
<thead>
<tr>
<th></th>
<th>Handwritten signature</th>
<th>Electronic signature</th>
<th>Digital signature</th>
<th>Digital certificate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contracts and agreements</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Employment documents</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Payroll documents</td>
<td>✓</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Standard drawings</td>
<td>*</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Design exceptions</td>
<td>*</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Plan sheets</td>
<td>*</td>
<td>x</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>All other documents</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

✓ = accepted  * = accepted only if exception is granted  x = not accepted

**Background**

The Utah Legislature enacted the UETA (UCA 46-4) during the 2000 General Session. The UETA does not require any state governmental agency to conduct transactions by electronic means or to use or permit the use of electronic records or electronic signatures except as provided in Subsection 46-4-301(6). The UETA does allow a state governmental agency to make rules to specify transactions that may be conducted by electronic means, transactions that will never be conducted by electronic means, the manner and format used for electronic communications, and the type of electronic signature required if law or rule requires that the electronic records be signed by electronic means.

**Definitions**

**Electronic signature**

An electronic sound, symbol, or process, attached to or logically associated with an electronic record and executed or adopted by a person with the intent to sign a record.
**Digital signature**
An electronic signature that can be used to authenticate the identity of the signer through password protection or other process

**Digital certificate**
A digital signature that uses Public Key Infrastructure (PKI) technology to guarantee signer identity

**PKI technology**
Basis for digital signature. PKI provides each user with a public key and a private key

**Private Key**
A value provided by a designated authority to be used by the signer to apply an electronic signature to a record

**Public Key**
A value provided by a designated authority as a key for others to use to validate the signer’s electronic signature and identity