

**DAS Statewide Policy**

**SUBJECT:** Identity Authentication/Electronic Signatures      **NUMBER:** 000-00-000  
**DIVISION:** IRMD - XX      **EFFECTIVE DATE:** 00-00-00

**APPROVED:** (Draft) Direct comments to Catherine Webber at DAS/IRMD

PURPOSE      The purpose of this policy is to provide guidance and standards for state agencies to implement the identity authentication and electronic signature provisions of the [Uniform Electronic Transactions Act](#) (UETA).

CONTEXT      UETA has been adopted by 49 states. Similar federal laws have also been enacted making UETA, in effect, national law.

UETA, adopted by Oregon in 2001, creates legal recognition for most electronic transactions and parallels the legal recognition provided for paper transactions conducted in Oregon.

UETA states:

- No transaction shall be denied legal effect or enforceability solely because it is electronic.
- A contract may not be denied legal effect or enforceability solely because it is in electronic format.
- If the law requires a record to be in writing, an electronic record satisfies that law.
- If a law requires a signature, an electronic signature satisfies that requirement.

UETA also:

- Provides guidance for Oregon parties conducting electronic transactions.
- Provides guidance for state agencies conducting electronic transactions.
- Directs the Oregon Department of Administrative Services (DAS) to develop guidelines and standards for state agencies conducting electronic transactions.

This policy applies only to the identity authentication and electronic signature requirements of UETA. Guidance for the other provisions of UETA relating to preservation, disposition, integrity, security, confidentiality and auditability of electronic records and transmission of electronic transactions will be provided in separate policy.

This policy does not directly apply to “*authorization*.” Authorization focuses on actions a party is permitted to take.

This policy does not directly apply to “*non-repudiation*” which is a technical concept relating to the level of proof or evidence that a transaction has not been compromised.

Policy:      State agencies shall use the following process, adapted from the federal E-authentication model, for electronic signatures and identity authentication in all UETA covered electronic transactions:

1. Use the federal [E-RA risk assessment tool](#) to conduct a risk assessment of the

## Statewide Operations Manual

**POLICY NAME**

**POLICY NUMBER**

- electronic transactions requiring authentication of remote users.
2. Map identified risks to the required assurance levels. Use the assurance model adopted by the federal E-authentication initiative to determine the acceptable risk level for the transactions and level of assurance to mitigate that risk.
  3. Select and implement tool and technology based on E-authentication technical guidance [NIST 800-63](#). Only products certified by NIST and approved by DAS may be used. When an Oregon E-authentication program is available, agencies applications whose requirements are met by the program will be required to use the program.
  4. Test the application after implementation to validate that the authentication system has operationally achieved the required assurance level.
  5. Reassess, periodically, to determine technology refresh requirements and changing business requirements for electronic authorizations. Take appropriate action.

The E-authentication process must comply with the agency's security plan, other state and federal laws including but not limited to Health Insurance Portability Accountability Act (HIPAA); Americans with Disabilities Act, Sarbanes-Oxley Act; Gramm, Leach, Blylie Act; Children's Online Privacy Act and laws specific to the implementing agency.

Software applications used to manage identity for electronic transactions shall protect personal identifiable information collected to authenticate:

- Publish state and agency privacy policy at the point personally identifiable information is collected for authentication.
- Restrict collection of information for authentication only to information that is necessary for authentication.
- Restrict the use of information collected for electronic authentication to authentication purposes.
- Include a statement how collected information will be used.
- Specify how long collected information will be retained.
- Provide a summary of the effect of public records law on the electronic transaction, if applicable.

State agencies may not require third parties to conduct transactions electronically. State agencies may direct employees to use electronic transactions when performing their work-related tasks.

### EXCEPTIONS:

State agencies that adopt authentication tools that are at a higher or lower level of assurance than indicated in the risk assessment process shall:

- Describe the reason for variance.
- Identify the potential risk of using a tool from a lower assurance level that the risk assessment identifies.
- Obtain the signed approval of the agency director.
- The signed document shall be available at (location) (approved by the director of DAS)
- Take necessary management steps to mitigate the risk.

State agencies that adopt software or tools that are not certified by NIST must obtain DAS approval prior to implementation for adopting a non-certified product.

## Statewide Operations Manual

### **POLICY NAME**

### **POLICY NUMBER**

#### GOALS:

The primary goal of this policy is to help Oregon achieve the benefits of digital government by:

- Enabling state agencies to develop and adopt electronic signing of documents and forms, and to creating procedures for the authentication of parties to transactions.
- Reducing costs related to paper transactions.
- Providing Oregonians, businesses and state employees the speed and convenience of conducting business 24/7/365.

A secondary goal of this policy is to increase state use of electronic transactions by reducing the risk of fraud and increasing the confidence of state agencies that remote parties to electronic transactions are who they represent themselves to be.

#### INTENT:

The intent of this policy is to have E-Authentication mechanisms that are practical and balance risk and cost. It is not the intent of this policy to eliminate all risk but rather to provide a process that gives parties assurance that the level of risk and mitigation tools used are reasonable for the type of transaction conducted.

Requiring authentication levels that are higher than the reasonable assurance levels can discourage use and unnecessarily increase cost to all parties. Levels too low fail to provide the assurance needed for parties conducting electronic business.

The intent of this policy is to have E-authentication systems provide an appropriate level of privacy protection for information collected to authenticate identity because without these assurances Oregon citizens, businesses and employees will not use the applications.

#### AUTHORITY:

[Uniform Electronic Transactions Act Chapter 84 \(HB 2112\)](#) generally and specifically §84.049, §84.052, §84.055, and §84.064 and [OAR 125-600-0000](#).

For overall authority of DAS See: [ORS 291.038](#) and [184.305](#).

#### EFFECTIVE DATE:

This policy effects:

- All new applications with electronic transactions using electronic signatures or identity authentication that are implemented after the effective date of this policy.
- This policy does not apply to electronic transactions in existence prior to the effective date of this policy.

#### APPLICABILITY:

This policy applies to:

- All state agencies including boards and commissions that use State Treasury for financial transactions.

This policy does not apply to:

- The Oregon Legislative Assembly, Courts and District Attorney Offices.
- Certain state agency transactions specifically excluded by UETA including those involving wills and trusts, the Uniform Commercial Code, and certain customer protection transactions.

#### ATTACHMENTS:

- [Attachment 1 - ERA Risk Management Tool](#) (Oregon version to be substituted)
- [Attachment 2 - NIST standards and list of certified vendors](#)
- Attachment 3 - Oregon Cookbook for implementing E-authentication (FYI: not

Statewide Operations Manual

**POLICY NAME**

**POLICY NUMBER**

- complete at this time)*
- Attachment 4 – Federal E-authentication policy (*feds will provide link in time for publishing*)