Trust Elevation

- Increasing the trust a relying party has that the online entity accessing its resources is the person or device it claims to be...

- Reducing the risk that a relying party assumes that the online entity accessing its resources is not the person or device it claims to be
Trust Elevation Core Model

User Accesses Online Resource with identity and/or attribute data (may consist of credential) [1, 2]

Resource Assesses Trustworthiness of Asserted Identity According to Policy [3, 4, 5]

Resource Determines Insufficient Trustworthiness [6]

Resource Engages Previously-Determined Trust Elevation Process [7, 8, 9, 10, 11, 12]

Rejection [13, 14]

Access resource for the transaction [13, 14]

Reapplication of yet another trust elevation cycle
Trust Elevation Technical Committee

Process

❖ Phase One/Deliverable One: Collect current and imminent trust elevation methods
❖ Phase Two/Deliverable Two: Analysis of collected methods
❖ Phase Three/Deliverable Three: General principles and techniques to elevate trust in a transaction
❖ Phase Four/Deliverable Four: Trust Elevation Markup Language
Trust Elevation Process Assertions

- Would support existing authentication and authorization specification but will remain independent of them.
- Would ensure existing identity assertion frameworks are supported
- Would be in XML and JSON formats
- Must be over SSL/TLS
Trust Elevation Sequence - Story

1. End-User accesses online resource using a device with an asserted identity and/or attributes.

2. Device sends End-User’s identity and/or attribute data to Relying Party (RP)

3. RP requests an Identity Provider (IdP) to assess the asserted identity.

4. RP validates each and every asserted attributes, if they are available, using an Attribute Provider (AP). The AP could be independent, part of RP or part of a third party. RP may involve multiple APs in a single transaction to validate various attributes.

5. RP engages LoA Assessor (LA) to assess LoA for the verified identity and/or attributes strength.

6. RP determines if the asserted identity and attributes offer sufficient trustworthiness. For sufficient trustworthiness, present the resource [13, 14]. For insufficient trustworthiness, follow Trust Elevation steps [7 - 12]. If there is no opportunity to elevate trust, then reject the request [13, 14]

7. RP engages Trust-Elevation Method Determiner (MD) to determine the best possible type of method be used for Trust Elevation. The MD is a repository of predetermined Trust Elevation methods for transactions involving various combinations of type of devices, RPs, IdPs, APs and LAs. The MD could be independent, part of RP or part of a third party.

8. RP, based on feedback from MD, requests valid authentication factors through the device. The device could provide factors with/without End-User Intervention.
Trust Elevation Sequence - Story

9. RP requests an Identity Provider (IdP) to assess the asserted identity.

10. RP validates each and every asserted attributes, if they are available, using an Attribute Provider (AP). The AP could be independent, part of RP or part of a third party. RP may involve multiple APs in a single transaction to validate various attributes.

11. RP engages LoA Assessor (LA) to assess LoA for the verified identity and/or attributes strength.

12. RP determines if the asserted identity and attributes offer sufficient trustworthiness. For sufficient trustworthiness, present the resource [13, 14]. For insufficient trustworthiness, follow Trust Elevation steps [7 - 12]. If there is no opportunity to elevate trust, then reject the request [13, 14]

13. RP presents information to device

14. Device present information to End-User
Trust Elevation – LoA Assessment

LA Request
<trustel:AssessLoaRequest>
  <trustel:AssertedID>...</trustel:AssertedID>  //could be SAML token
  <trustel:AssertedAttribute>
    <trustel:Attribute>...</trustel:Attribute>  //Attribute
    <trustel:AttributeProvider>...</trustel:AttributeProvider>  //AP OU
  </trustel:AssertedAttribute>
  <trustel:AssertedAttribute>
    <trustel:Attribute>...</trustel:Attribute>  //Attribute
    <trustel:AttributeProvider>...</trustel:AttributeProvider>  //AP OU
  </trustel:AssertedAttribute>
  <trustel:Loa>...</trustel:Loa>  //current LoA Strength in numerical value
  <trustel:LoaAssessor>...</trustel:LoaAssessor>  //LoA OU
  <trustel:AuthnContext>
    <trustel:AuthnDeviceSig>...</trustel:AuthnDeviceSig>  //Device Fingerprint
    <trustel:AuthnLocation>...</trustel:AuthnLocation>  //Device location
    <trustel:AuthnIP>...</trustel:AuthnIP>  //IP of the device
    <trustel:AuthnTime>...</trustel:AuthnTime>  //time of request
  </trustel:AuthnContext>
</trustel:AssessLoaRequest>

LA Response
<trustel:AssessLoaResponse>
  <trustel:AssertedID>...</trustel:AssertedID>  //could be SAML token
  <trustel:LoaStrength>...</trustel:LoaStrength>  //could be numerical value
  <trustel:LoaAssessor>...</trustel:LoaAssessor>  //LoA OU
  <trustel:LoaAssessorSig>...</trustel:LoaAssessorSig>  //LoA OU Signature
</trustel:AssessLoaResponse>
Trust Elevation – Method Determination

**MD Request**

```xml
<trustel:MethodTypeRequest>
  <trustel:AssertedID>...</trustel:AssertedID>  //could be SAML token
  <trustel:AssertedAttribute>
    <trustel:Attribute>...</trustel:Attribute>  //Attribute
    <trustel:AttributeProvider>...</trustel:AttributeProvider>  //AP OU
  </trustel:AssertedAttribute>
  <trustel:AssertedAttribute>
    <trustel:Attribute>...</trustel:Attribute>  //Attribute
    <trustel:AttributeProvider>...</trustel:AttributeProvider>  //AP OU
  </trustel:AssertedAttribute>
  <trustel:Loa>...</trustel:Loa>  //current LoA Strength in numerical value
  <trustel:LoaAssessor>...</trustel:LoaAssessor>  //LoA OU
  <trustel:AuthnContext>
    <trustel:AuthnDeviceSig>...</trustel:AuthnDeviceSig>  //Device Fingerprint
    <trustel:AuthnLocation>...</trustel:AuthnLocation>  //Device location
    <trustel:AuthnIP>...</trustel:AuthnIP>  //IP of the device
    <trustel:AuthnTime>...</trustel:AuthnTime>  //time of request
  </trustel:AuthnContext>
</trustel:MethodTypeRequest>
```

**MD Response**

```xml
<trustel:MethodTypeResponse>
  <trustel:AssertedID>...</trustel:AssertedID>  //could be SAML token
  <trustel:Method>...</trustel:Method>  //could be "|" delemited array of methods
  <trustel:MethodDeterminer>...</trustel:MethodDeterminer>  //MD OU
  <trustel:MethodDeterminerSig>...</trustel:MethodDeterminerSig>  //MD OU Signature
</trustel:MethodTypeResponse>
```
Trust-El Use Case 1

Diagram:
- End User
- Device
- Relying Party (RP)
- Identity Provider (idP)
- Attribute Provider (AP)
- LoA Assessor
- Trust-El Method Determiner
Trust-El Use Case 2
Trust-El Use Case 3