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
User Accesses Online Resource with identity and/or attribute data (may consist of credential)

Resource Assesses Trustworthiness of Asserted Identity According to Policy

Resource Determines Insufficient Trustworthiness

Resource Engages Previously-Determined Trust Elevation Process

rejection

access resource for the transaction

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

- **Sources:** TC Membership

- **General Disregarded Whines**
  - Too much NIST (X.1254 is baseline)
  - Credential vs. Transactional (Process works for both)
Phase Three Document

- Skeleton formed from these elements:
  - A methodology for aligning various different trust models
    - Increased trust in an asserted online identity = increased mitigation of risk of fraud, etc.
    - Ergo, trust elevation = risk mitigation
  - A benchmark
    - Risk vector based, international
  - A tool for associating the trust models against the benchmark and cross-walking requirements among different trust models
    - The Table
  - A recommendation for what constitutes trust elevation
    - Based on how multi-factor authentication works
## Graphic

<table>
<thead>
<tr>
<th>Methodology: Risk Vectors Mitigation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Benchmark: X.1254 List of Risk Vectors</td>
</tr>
<tr>
<td>Recommendation: What elevates trust?</td>
</tr>
<tr>
<td>Tool: The Table</td>
</tr>
</tbody>
</table>
Methodology for Recommendation

Because the set of risk vectors is more or less common to all Identity Management standards and frameworks (only the associated analysis and controls processes differ), the TC chose to use the ITU-T X.1254 catalog of risk vectors as the standard list and to prune them down to only those affecting authentication risks.

This list is the baseline against which the trust elevation methods have been arrayed in the Table.
Recommendation on Trust Elevation Implementation

Based upon an assessment of the state of the art by the TC membership, trust in the transaction is increased by what may be comparable to one NIST LoA when one trust elevation technique satisfies either of the following criteria:

- The technique mitigates a different threat vector — e.g., implementing an additional factor which doesn't share the same vulnerability as the factors previously engaged, or
- The technique leads to increase in confidence in an existing factor by enhancing a mitigation strategy that has been applied previously.
Why Should You Care?

- Creates a generalizable framework for implementing non-credential-based, online authentication best practices based on current and near-future implementations
  - Hence extensible to current FS audited practices and modifiable as new approaches to mitigating risks appear
- Expands and extends options for multi-factor authentication implementations
- Creates a normalized methodology for evaluating and mapping both credential-based and non-credential-based authentication practices of external trust frameworks
  - Enables trusted interoperability at the RP policy level
- Existing system may be impacted if this framework is extended to a trust elevation standard perhaps in XML) in the future and the impact would be on identity providers, trust elevation systems, and relying parties
Contacts for Comments and Further Discussion

- **Abbie Barbir**, Bank of America: abbie.barbir@bankofamerica.com
- **Steve Olshansky**, for the TC: steveo@luminagroup.com
- **Peter Alterman**, SAFE-BioPharma Assn.: palterman@safe-biopharma.org