Identity Assurance Framework

Executive Summary

Assurance of a user's identity in an electronic system is required for many University business processes to function efficiently and effectively. As the risk associated with an electronic system increases (whether the risk is financial loss, loss of reputation, damage to University programs, etc.), the required level of assurance in the identity of the user of the system also increases.

Level of assurance is the product of identity administration processes (such as identity proofing, credential issuance, etc.) and electronic authentication processes (such as password-based authentication, two-factor authentication, etc.).

Since August 2006, the University has had a two-tier level of assurance system – a basic level of assurance and an upgraded level of assurance. These two tiers no longer meet the business needs of the University and a more granular set of assurance levels is needed to provide both a lower level of assurance for low-risk systems and a higher level of assurance for high-risk systems.

This Identity Assurance Framework (IAF) describes a new level of assurance system along with a risk assessment process that University departments can use to determine which authentication options are appropriate for their systems.

The IAF is part of the Identity and Access Management (IAM) Roadmap, a series of initiatives to improve the capabilities of the University's IAM infrastructure and address key business needs.

Levels of Assurance

Current Levels of Assurance

The University's UT EID system currently has two levels of assurance, basic and upgraded. All UT EIDs are created at the basic level. Basic level UT EIDs usually have self-asserted identity information, though in some cases University systems of record may provide identity information for these UT EIDs. To reach the upgraded level, the identity holder must have an eligible formal relationship with the University (for example, student, faculty, staff, retiree, official visitor, etc.), complete an in-person identity proofing process, and sign the University's Electronic ID Agreement. Upgraded UT EIDs are generally required for online processes that would require a physical signature if they were performed offline. Two-factor authentication has been added to specific online processes to provide additional identity assurance beyond the normal "upgraded" level.

With the addition of two-factor authentication and the upcoming introduction of "lightweight" authentication accounts (to facilitate online interactions with loosely

affiliated populations), the University has outgrown the existing two-level level of assurance framework. Campus units need an enhanced level of assurance framework that provides clear guidance for selecting appropriate authentication options for their systems.

New Levels of Assurance

In the new level of assurance framework, shown in Table 1 below, identity assurance ranges from "Low" at Level 0 to "Very High" at Level 3 (or "Exceptionally High" at Level 4, if needed in the future). As the level of assurance increases, more robust identity vetting and stronger authentication are required.

Table 1: Levels of Assurance

Level	Identity Assurance	Typical Authentication Experience	Sample Usage
Level 0	Low	Lightweight or social identity	• Registering for a campus visit • Signing up for an alumni event
Level 1	Moderate	Lightweight or social identity with identity vetting* UT EID with identity vetting	• Accessing admissions status • Checking donation history • Completing pre-employment processes
Level 2	High	Upgraded UT EID**	• Registering for classes • Completing employee timesheets
Level 3	Very High	Upgraded UT EID plus two-factor authentication	• Updating paycheck direct deposit routing • Accessing application administrative functions from off-campus
Level 4 (Future)	Exceptionally High	TBD	TBD

* Identity vetting means that a trusted University department has confirmed information associated with an identity account, such as name, email address, etc.

** Upgraded UT EID means that the user has completed in-person identity proofing (also known as the "IDP" entitlement) and has signed the University's Electronic ID Agreement ("SIG" entitlement).

Selecting a Level of Assurance

The appropriate level of assurance for an online system can be determined using a three-step process:

- Step 1: Assess risks.
- Step 2: Determine required level of assurance.

- Step 3: Select an appropriate authentication option.

Using this 3-step process, campus departments can evaluate the potential impact of an authentication failure in a particular system, determine the level of assurance needed, and identify which authentication options are available to provide that level of assurance.

The primary responsibility of identifying the proper level of assurance for a system lies with the system owner since they best understand the business process their system supports, the system's users, and the potential impact of an authentication failure in the system.

As campus departments assess their systems, they should consider whether different user groups within that system have greatly differing risk profiles. This may result in a particular system requiring different levels of assurance depending on the user type. For example, if a system has a self-service view that only allows the user to view their own data and an administrative view that allows authorized users to see many people's data, the self-service part of the system *may* have a lower level of assurance requirement than the administrative part. Since costs, complexity, and user inconvenience increase as the level of assurance goes up, system owners should strive to use the lowest level of assurance appropriate for their systems.

Step 1: Assess Risks

What is the potential impact of an authentication failure in my system?

An authentication failure occurs when one user is able to authenticate as another user. For example, if an EID holder falls for a phishing scam and unknowingly provides their EID password to the phisher, and the phisher uses that password to log on as the EID holder, an authentication failure has occurred.

Authentication failures in an electronic system can pose a variety of risks, including:

- Inconvenience, distress, or damage to University standing or reputation
- Financial loss or University liability
- Harm to University programs or public interests
- Unauthorized release of sensitive or confidential information
- Civil or criminal violations
- Personal safety

The overall risk level of an authentication failure depends on the potential severity of harm posed by the risk and the likelihood that the risk will occur. Risk assessments should consider a wide range of impacts based on the business processes, policies, data, and technologies that are within the system's control.

In Step 1, the system owner will rate whether the system poses a low, moderate, or high risk in six risk areas. It is possible that a risk area may not be applicable to an application. For example, a system may pose a high risk for financial loss but may not involve any risk to personal safety.

Table 2 below provides the corresponding criteria for assessing the risk severity for each of the risk areas.

Table 2: Determining Risk Levels

Risk Area	Low Risk	Moderate Risk	High Risk
Inconvenience, distress, or damage to University standing or reputation	Local media attention quickly remedied. Reportable incident to Department Head with no follow up. Isolated faculty, staff, or student dissatisfaction.	National short-term media coverage. Reportable incident to University Administration with immediate correction. Widespread morale problems and high turnover.	International long-term media coverage. Reportable incident to Board of Regents requiring major project for corrective action. High turnover of experienced staff. University not perceived as employer of choice.
Financial loss or University liability	No or minimal loss of revenue or fraud. No adjustment needed to previous financial statements. No impact on external credit ratings.	Significant financial loss of revenue triggers audit. Minor adjustment needed to previous financial statements. Minor impact on external credit ratings.	Material loss of revenue. Previous financial statements require third-party review. External credit agencies drastically lower ratings.
Harm to University programs or public interests	Minor adverse effect on University programs, operations, assets, or public interests. University is able to perform its primary functions but effectiveness of the functions may be reduced.	Major adverse effect on University programs, operations, assets, or public interests. Effectiveness of University functions are significantly reduced.	Severe effect on University programs, operations, assets, or public interests. University is not able to perform one or more of its primary functions.
Unauthorized release of sensitive or confidential information (i.e. Student, Patient, Donor/Alumni, Research, Employee, Business/Vendor, and Institutional Data)	Released data includes less than 2 of the confidential data categories defined by ISO.	Released data includes 3-5 of the confidential data categories defined by ISO.	Released data includes more than 5 of the confidential data categories defined by ISO.
Personal safety	Minor injuries to employees or third parties.	Outpatient medical treatment required for employees or third parties.	Significant injuries or fatalities to employees or third parties.

Civil or criminal violation	No reportable civil or criminal violations.	Civil or criminal violations that may be subject to state enforcement efforts.	Civil or criminal prosecution or fines, litigation including class actions at federal level.

Step 2: Determine Required Level of Assurance

What assurance level should my application adhere to?

The risk levels determined in Step 1 are mapped by risk area to specific levels of assurance (see Table 3 below). In some risk areas, such as personal safety, even a low risk may require an elevated level of assurance.

The highest level of assurance identified in this mapping for a particular system determines the overall level of assurance required by that system. It is the responsibility of the system owner to select the appropriate level of assurance needed for their system since they are most familiar with their business processes and associated risks.

Table 3: Mapping Risk Level to Level of Assurance

Risk Area ↓ Risk Level →	None or n/a	Low	Moderate	High
Inconvenience, distress, or damage to University standing or reputation	Level 0	Level 1	Level 2	Level 3
Financial loss or University liability	Level 0	Level 1	Level 2	Level 3
Harm to University programs or public interests	Level 0	Level 1	Level 2	Level 3
Unauthorized release of sensitive or confidential information	Level 0	Level 1	Level 2	Level 3
Personal safety	Level 0	Level 2	Level 3	Level 3
Civil or criminal violation	Level 0	Level 2	Level 3	Level 3

To comply with UT System policy[1], if either of the following situations applies, Level 3 will be required, even if the risk mapping indicates a lower level of assurance:

a) an employee or other individual providing services on behalf of the University (such as a student employee, contractor, or volunteer) logs on to a University network using an enterprise remote access gateway such as VPN, Terminal Server, Connect, Citrix, or similar services;
b) an individual described in (a) who is working from a remote location uses an online function such as a web page to modify employee banking, tax, or financial Information; or

[1] See UTS165: http://www.utsystem.edu/offices/board-regents/uts165-standards#s4

c) a server administrator or other individual working from a remote location uses administrator credentials to access a server that contains or has access to confidential University data.

Step 3: Select an Appropriate Authentication Option

What are my authentication options to achieve the required level of assurance?

There are various centralized authentication options that satisfy the requirements for each level of assurance, as described in Table 4 below.

Table 4: Authentication Options

Level of Assurance	Authentication Requirements	Authentication Options
Level 0	• Lightweight or social identity -OR- • UT EID	• Lightweight Authentication • UTLogin • Shibboleth • LDAP (TED/AD)
Level 1	• Lightweight or social identity, with identity vetting* -OR- • UT EID with identity vetting	• Lightweight Authentication with identity vetting • UTLogin • Shibboleth • LDAP (TED/AD)
Level 2	• Upgraded UT EID**	• UTLogin with check for IDP & SIG entitlements • Shibboleth with check for IDP & SIG entitlements • LDAP (TED/AD) with check for IDP & SIG entitlements
Level 3	• Upgraded UT EID -AND- • Two-factor authentication	• UTLogin with check for IDP & SIG entitlements and two-factor authentication enabled • Shibboleth with check for IDP & SIG entitlements and two-factor authentication enabled
Level 4 (Future)	TBD	TBD

* Identity vetting means that a trusted University department has confirmed information associated with an identity account, such as name, email address, etc.

** Upgraded UT EID means that the user has completed in-person identity proofing ("IDP" entitlement) and has signed the University's Electronic ID Agreement ("SIG" entitlement).

Implementation

Implementation of this Identity Assurance Framework will involve work in several areas. Planning for this implementation work will occur during the spring of 2016.

- **Assurance Level Assessment Tool** – An assessment tool will be developed to help campus departments select an appropriate level of assurance. This could

take the form of an online questionnaire or other tool that guides the department through the process and provides them with clear guidance on which level of assurance is needed for their system and how they can satisfy it.

- **Identity Vetting Process** – The IAM Team will define a central identity vetting process used with Level 1 assurance. The source information about an individual will be collected from a University department's business process. The process will collect name, date of birth, phone number, and a verified email address. These four pieces of information will be the baseline of information required for generating the account and obtaining a password reset. Once the department has a process in place to verify email addresses and provide confirmation to the IAM Team, the department will become a trusted department.

  The identity vetting process will be flexible to accommodate systems of differing risks. Any system that possesses a higher risk but does not constitute a Level 2 assurance will require additional checks based on other incidental information collected by the University. For example, if a user has donated to the University, the department has their validated billing information and this information could be used to vet the user as long as the incidental data was made available to the IAM Team. If departments want to create their own linkages between local accounts and social accounts for higher risk systems not requiring Level 2 assurance, the user will have to agree to take on that risk when their billing information is validated. The departments collecting this information will need to add disclaimers about how the information collected will be used.

- **Coordination with Related Projects** – Two other IAM Roadmap projects have close relationships with identity assurance: Lightweight Authentication and Multi-Factor Authentication. The implementation of the new capabilities provided by these projects will be aligned with the Identity Assurance Framework.

- **Communication and Education** – A communication and education campaign will be needed to introduce the new level of assurance structure and risk assessment process to campus stakeholders, including both the technical and business communities. Specific technical instructions will be developed to explain to the campus technical community how to configure the available authentication tools in their different system environments in order to satisfy the requirements for a particular level of assurance. The IAM Team will consider the legacy systems' roadmaps and will work with the system owners to agree on the best approach and timeline to implement the IAF that reduces the amount of rework required.

- **Level of Assurance Compliance** - A process is needed to ensure that the level of assurance selected is still appropriate to the evolving business needs supported by the systems. The process will require the system owners to conduct risk assessments of their systems similar to the Information Security Office Risk Assessment (ISORA) and reassess their current level of assurance on a yearly basis. The IAM Team and ISO may enforce the framework by performing audits

of the authentication option implemented to ensure that it is consistent with the selected assurance level and complies with UT System policy (UTS165). ISO audit results and further risks analysis may trigger the need for an additional identity assurance level in the future.

- **IAF Change Management -** After the Identity Assurance Framework (IAF) has been implemented, any changes to the framework including the identity vetting process will be prioritized and submitted for approval to the IAM Committee. It is the responsibility of the IAM Team to maintain the IAF up to date with the latest authentication options and risk levels. The IAM Team plans to find two-factor and lightweight authentication early adopters in order for them to provide feedback on the overall process before a broad rollout of the IAF to the University.

Appendix 1

Table 5: Case Studies

No.	Name	Problem/Challenge	Resolution
1	Prospective Student Campus Visit Sign Up	Prospective students used to sign up for campus visits and other recruiting events on a site hosted on UT Direct which required UT EID authentication. The Admissions Office found that the UT EID creation process acted as a deterrent to prospective students who were casually surfing for information and did not want to go through what seemed like a very "official" process of creating a UT EID to sign up for campus visits.	The Admission Office now uses a vendor product to authenticate for certain actions such as registering for an event or a campus tour by just providing email address and password. However, the downside is that the burden of customer support for login issues such as locked accounts falls on the Admissions staff. With IAF, the Admission Office would have been guided to determine the appropriate level of assurance and selected the lightweight authentication option. Using the IAF would have saved the Admission Office the cost for the vendor product and the hours spent resolving login issues.
2	Payroll Phishing Attacks	Various phishing attacks impersonating established University units such as Payroll have been reported. The phishing attacks ask the user to click on a link which will prompt the user to enter their EID and password and will save their credentials to later access personal and sensitive data including email, bank deposit info, tax info, etc.	In the future, University departments will be able to assess their risk upfront and select the most efficient and effective authentication option. In the case of Payroll systems that allow updates to bank deposit information or tax information, the IAF would have indicated that assurance Level 3 was required and that two-factor authentication was needed. Implementing two-factor authentication would have prevented the financial loss of rerouting checks to the wrong hands.