Operational Challenges in deploying Trust Management Systems - A practical perspective

Dr. Sundeep Oberoi

Global Head – Niche Technologies Delivery Group
Tata Consultancy Services Ltd.
sundeep.oberoi@tcs.com

Extended Abstract

With the exponentially increasing number of transactions being performed online, it has become critical to ensure that any electronic transaction can be associated with the electronic persona who has carried out the transaction. Furthermore it is very important to ensure that this electronic persona can be associated with a real human persona. This need has been highlighted by the regularity with which security measures are breached. In the circumstance of a breach or a failure of security, it is very important to determine the real person associated with the transaction in question so that accountability can be fixed and appropriate follow up actions taken. This requirement of accountability must be fulfilled with the same degree of rigour that we are used to in traditional paper based systems where transactions are authorized and accountability fixed by the use of "wet" signatures. Unless we are able to practically achieve this same level of accountability in electronic systems, reliance on paper based systems will continue.

Associating a transaction with a real human person has two steps. First the transaction must be associated with an electronic identity. The most simple example of this is a user-name. The second step is associating the given electronic persona with a real human persona. This is usually a matter of policy although there are some technologies, like biometrics, which could help establish this association is deployed carefully. Both these associations must be made with the requisite level of rigour if they are to be used as the basis for accountability.

1 Associating Electronic Identities with Transactions

In order to associate an electronic identity with a transaction, the system must store the identity as a part of the transaction in some way. This could be manifest, i.e. a user name is stored as part of the transaction. Some systems may create session or transaction identifiers which can be associated with an electronic identity via log entries. In this case the association is inferred. In any properly designed system, it must be possible to associate each transaction with an electronic identity. Further is must not be

possible for this association to be altered by any means. Even if it is possible to identity an electronic identity in relation to each transaction and there is reasonable assurance that this identity has not been changed, it is still required to establish that the transaction was carried out by the person authorized to use that electronic identity. This is usually achieved by authentication.

In practical scenarios authentication may not be fine grained. Authentication might happen at the level of logon. In recent times online banking systems have increasingly begun to authenticate each transaction that transfers value. However barring such examples authentication remains largely coarse grained and most systems lack the integrity mechanisms to ensure that the identity association and fact of authentication are maintained in a manner that cannot be tampered with.

In this context many countries have adopted Electronic Signature legislation in order to standardize and increase the assurance that transactions may be reliably associated with electronic identities and that it may be established that the authorized bearers of those electronic identities actually authorized those transactions. The practical issues here are that

- These techniques may have to be retrofitted to systems which do not have a fine grained transaction authorization mechanism. This could have an impact on code as well as storage since the signature information may now have to be stored and in some way associated with the transaction.
- Not all electronic signature techniques can guarantee the integrity of the signed records. Thus trust is required in the policies under which these records are processed and stored.
- Electronic credentials may be stolen and used without the knowledge of the authorized holder of those credentials thereby casting doubt on the intent by the authorized holder to authorize the transaction in question.

In practical systems today there are a very large number of users. The user base and therefore user credentials is not common across even all applications being run by a particular organization, let alone across organizations. In this scenario it is unavoidable that some form of self service be provided in terms on allowing the user to generate credentials on their own after an initial verification. Thus although initial registration will require a lot of information and a password will be generated by a means under the control of an application owner, subsequent password resets are usually self service based on authentication against pre-registered information. While this appears to be a practical necessity, trust in such systems requires the rigorous application and constant monitoring of compliance to policies.

2 Associating a Human Persona with an Electronic Persona

Most traditional systems did not even attempt to do this. The systems worked at the level of issuing electronic identities to people and did not have any technical measures or policies that would generate assurance in the association of humans to their electronic identities.

With the increasing adoption of electronic signature legislation it is becoming increasingly important to have high assurance in associating a given electronic identity to a specific individual. This requires that the identity of an individual requesting an electronic credential be rigorously verified before the electronic credential is issued. The practical problems here are

- Identity verification is expensive and inconvenient since a face to face verification might be required
- In light of the cost, practicality demands that such credentials be widely usable
- Applications must be in a position to use these interoperable credentials
- There must be ways to ensure that a credential can only be used by the authorized holder of the credential

The practical problems faced in deploying such systems have been

- Government Mandates needed when user base is not large enough
- Use seen largely as a compliance measure
- High verification costs which lead to lack of rigour in the credentialing process
- Insufficient measures to control unauthorized use of credentials

3 Summary

Although certain good technologies like Digital Signature and Biometrics exist that are technically secure, operating such technologies at a large scale requires trust management processes if their use is to be considered reliable and achieve the level of accountability that we expect from our traditional paper based system. This aspect of ensuring that a specific human persona is associated with a given electronic persona is a very vital element in ensuring the trustworthiness of electronic systems. Currently there are practical challenges in terms of cost and convenience which must be overcome before these systems can scale and be adopted widely.